California Year 2000

Desktop Systems

Program Guide

June, 1998

John Thomas Flynn
State Chief Information Officer
DEPARTMENT OF INFORMATION TECHNOLOGY
801 "K" Street, Suite 2100
Sacramento, CA 95814
Phone: 916.445.5900
Fax: 916.445.6524
www.year2000.ca.gov

California Year 2000 Desktop Systems Program Guide

Contents

Appendices

Tables

Figures

Acknowledgments

The *California Year 2000 Desktop Systems Program Guide* represents the efforts of many people. The DOIT wishes to acknowledge the assistance of those who have contributed to the development of this program by participating in the Year 2000 Embedded Systems Task Force and its Desktop Systems subcommittee.

Year 2000 Embedded Systems Task Force

Walt Barr	Department of Health Services
Jerry Beaman	Department of Mental Health
John Bowles	Office of Emergency Services
Jack Connell	CTA Incorporated
Jerry Cottrell	Department of Finance
Mike Courtney	Department of General Services – Real Estate Services
Joyce Fong	Public Utilities Commission
Toni Frederickson	Department of Forestry & Fire Protection
Angela Garvi	Department of Health & Welfare Agency Data Center
Michael Goble	Department of General Services – Real Estate Services
Susan Hancock	Department of Corrections
Larry Hoffart	Department of Industrial Relations
Bob Jordan	Department of Water Resources
Mike Kanemoto	Department of Justice – Hawkins Data Center
Michael Lucas	DynCorp Management Resources
Dana McIntyre	CTA Incorporated
John McMahon	California Highway Patrol
John McMillan	Department of Transportation
Leslie Medina	DynCorp Management Resources
Russ Ogata	Sacramento County Public Works
Debra Reiger	Department of Health & Welfare Agency Data Center
Dennis Russell	Stephen P. Teale Data Center
Linda Sanford	Department of Consumer Affairs
Elmer Schau	Stephen P. Teale Data Center
Allan Tolman	Department of General Services – Telecommunications
Doug Yee	Department of Developmental Services

Department of Information Technology

John Thomas Flynn
Ron Ridderbusch
Claudina Nevis
Janice Barnett
Rita Champlion

EXECUTIVE SUMMARY

In November 1996, the Department of Information Technology (DOIT) issued the *California 2000 Program Guide,* providing the State's Information Technology (IT) organizations with a methodology and reporting process for remediating IT **mission critical** systems. Two potential Year 2000 (Y2K) problem areas were not directly addressed within that guide: embedded systems and desktops. Embedded systems are the subject of a separate DOIT publication, issued in June 1998. This publication, the *California Year 2000 Desktop Systems Program Guide*, addresses the State's Y2K program for desktop microcomputers and related network infrastructure.

Focus

The *California Year 2000 Desktop Systems Program Guide* presents a methodology for remediating desktop systems that support *necessary* business systems. *Necessary business functions* are defined as those that affect an organization's ability to perform its required or essential functions. All desktop-based mission critical business functions are assumed by the DOIT as having been previously addressed through the *California 2000 Program Guide*.

The *California Year 2000 Desktop Systems Program Guide* focuses on the identification, prioritization, and remediation of **computing hardware**, **operating systems software**, and **applications software** within the desktop environment. The desktop environment in this context includes:

- Desktop, Laptop and/or Client Personal Computers
- Server Computers
- Desktop Operating Systems
- Network Operating Systems

Areas beyond these specific boundaries have been or are being addressed through previous or current DOIT publications.

This Program Guide provides an overview of the California 2000 Desktop Systems Program. The Program Guide is intended to assist the State's Year 2000 efforts through:

- Dissemination of a common methodology or approach for prioritizing desktop Y2K issues to be used by State departments
- Identification of commercial and public domain tool sets for the efficient inventory, assessment, remediation, and testing of the affected environments

The Problem

The desktop millennium bug is a complex problem that may affect the interaction of computer hardware, operating system software, application software, and data files, such as spreadsheets. These systems are the ones we rely upon every day – personal computers (PCs) for word processing and spreadsheet work, Local Area Networks (LANs) that support file printing and data transfers, and servers that house the data and applications that we share. A failure in one of these systems, or potentially, corruption of shared data within a server or LAN environment, may cause impaired or ineffective service to the public.

The State of California possesses thousands of desktop, laptop, and server computers, spread widely across the state. Desktop systems and the LANS supporting those systems range in size from single, stand-alone PC systems, to large multi-server LAN environments with hundreds of client PCs. Because of this complex environment, the logistics and management issues for dealing with the desktop Y2K problem are very complex.

The Impact

California State agencies and departments purchase desktop hardware and software from a variety of mechanisms, including, but not limited to, the State Computer Store, the California Multiple Award Schedule, and other purchasing mechanisms. There is no single source for information related to the total number of desktop hardware and software products purchased throughout the State. Even though comprehensive data is not available, we know that the State is a significant purchaser of desktop computer products. For example, information provided by the State Computer Store suggests that thousands of desktop computer products have been procured over the past two years. Clearly, the number of these products statewide is enormous, as is the potential for negative side effects.

Below are just two examples of the effects desktop Y2K problems may have on any particular department.

Errant date information in one spreadsheet may seem a minor issue, but if that data is shared by other applications, or interfaced with other environments, an incorrect date can quickly spread. Incorrect date information that is innocuous in one environment may be critical within another. For example, consider incorrect date information being rolled up into a medical claims processing system, wherein access to needed health care is falsely denied.

Similarly, the failure of one desktop to pass the correct date to a spreadsheet may seem an isolated one, but the ramifications of a server doing the same expands the impact. Incorrect dates on reports are of little consequence with an informed readership, but database or spreadsheet calculations deriving inaccurate or incorrect results are of greater potential impact. For an example of the potential problems, consider the ramifications of an incorrectly calculated benefits check, due entirely to date inconsistencies within a database.

The Solution

In recognition of the Year 2000 problem in the desktop environment, DOIT recommends state agencies and departments do the following:

- Conduct a risk assessment to identify necessary business functions
- Inventory desktop systems supporting the necessary business functions
- Prioritize the order of remediation, based upon the prioritized inventory
- Assess the Y2K compliance of the prioritized inventory list
- Determine the remedy for noncompliant systems/products
- Remedy the noncompliant systems/products
- Validate Y2K compliance through testing
- Plan for contingencies of noncompliant-induced system flaws or failures

This approach is detailed in the following pages.

Published Resources

The California Year 2000 Program comprises multiple subprograms focused on particular types of systems, each susceptible to the Year 2000 problem:

Y2K SubProgram	System Type Addressed
California Year 2000 Program Guide	Traditional IT systems.
California Year 2000 Embedded Systems Program Guide	Embedded technology/microprocessor systems/non-IT systems, including telecommunications systems and wide area network infrastructure.
California Year 2000 Desktop Systems Program Guide	Microcomputers and related network infrastructure, including file servers, local area networks, and desktop computers.
California Year 2000 White Paper: External Interfaces	External Interfaces coordination, synchronization and management issues.

SECTION 1: OVERVIEW OF THE PROBLEM

The problem within the desktop infrastructure can be broken down into three component areas: **desktop computing hardware** (stand-alone or client PCs, laptops, and servers), **operating system software**, and **application software** systems. For review of considerations beyond these issues, please refer to the California 2000 Embedded Systems or Information Technology Program Guides.

The desktop environment faces many potential Y2K problems:

- Desktop Computing Hardware (stand-alone, client, laptop, and server computers)
  - Basic Input Output System (BIOS)
- Operating Systems Software
  - Desktop Operating Systems
  - Network Operating Systems
- Application Software
  - Commercial Off-the-Shelf Software
  - Custom Developed Software

The failure or corruption of any one of these desktop-related components could cause the failure of a necessary business function. The potential failure of each of these components must be examined and addressed in relationship to the necessary business processes.

Problems in the desktop area are pervasive. For example, as late as May 1997, some of the desktop products being sold through the State Computer Store were noncompliant. Figure 1.1 portrays this one-month sampling of data from State Computer Store sales. Sales compliance data for products from the top ten hardware vendors in that month reveals that 5 percent of the products were noncompliant, with 9 percent requiring patches or manual intervention.

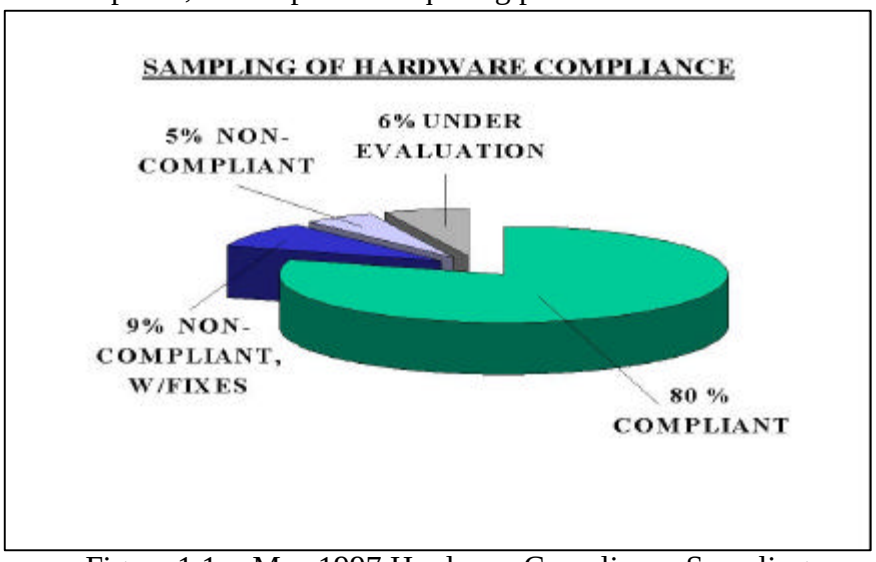

Figure 1.1 - May 1997 Hardware Compliance Sampling

Within the same one-month period, 13 percent of the software being sold through the State Computer Store was noncompliant, with an additional 12 percent requiring software patches (see Figure 1.2).

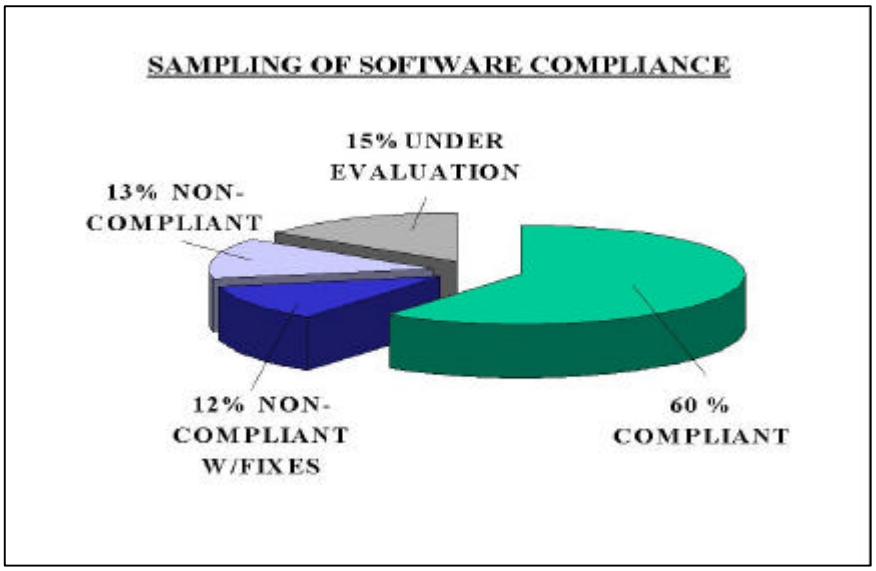

Figure 1.2 - May 1997 Software Compliance Sampling

Y2K managers should be careful not to assume that relatively new hardware and software products are Y2K compliant. All desktop infrastructure supporting necessary business functions should be examined, irrespective of purchase or production date.

Desktop Computing Hardware

The hardware issues affecting stand-alone or client desktop computers, laptops, and servers are basically the same: Basic Input Output System (BIOS). Network hubs and interface cards do not embody sufficient intelligence to perform any date functions, so they are not impacted by Y2K issues. Remediation of the BIOS problem, from the hardware perspective, can be achieved through the use of the same overall approach. Differences in application of the approach for each type of hardware (server versus client for example) may appear in certain stages of the process.

For example, client-type desktop and portable computing devices can be readily isolated from the network to allow for discrete testing and remediation of hardware-related issues. A client machine can be brought off-line from a network for testing with little impact to the overall environment. The same is not true for servers. Servers must be taken down in a way that will not impact the network. Additional testing complications arise when dealing with multi-segment LANs requiring date and time synchronization.

Operating Systems Software

Operating systems (OS) are strategic in their position relative to the desktop Y2K problem. They capture the date from the BIOS, and pass that date to application software. Should that date be errant as a result of incorrect calculation of the century change at the BIOS level, application

software may receive the OS date and replicate the problem. Noncompliant operating systems, whether installed on desktop computers or on servers as network operating systems (NOS), can be addressed through the same mechanism: software patch, upgrade or replacement.

Desktop Operating Systems

Noncompliant operating systems on the desktop will cause resident application software reliant upon the OS for dates to calculate or sort incorrectly. Disruptions in normal business practices may arise if important calculations and reports require manual verification (in benefits calculations, for instance).

Network Operating Systems

Special focus should be paid to ensure the compliance of NOSs because of their critical function in supporting a multitude of business systems. LAN-based business software, internal e-mail software, and the like are totally dependent upon a functioning NOS. A noncompliant NOS may not cause a cessation in dependent daily operations, but would most certainly disrupt the applications software dependent upon a correct baseline date. Fortunately, most currently supported LAN operating systems are Y2K compliant in their current release form.

Application Software

Application software is potentially the most difficult of the desktop Y2K problem areas because of the sheer number of commercial-off-the-shelf (COTS) applications installed, the number of variants of those packages, and the number of installed custom applications. The level of effort required to remediate the noncompliant packages will likely dwarf the efforts in the hardware and operating systems problem areas combined, because of the tremendous range and breadth of the applications software.

COTS Software

Many COTS products are standardized throughout the State, especially office suite products, but many are specialized to suit a particular organization's purpose. The most important aspect in remediating the COTS product base may well be a proper prioritization of systems requiring remediation. Upgrade or replacement cost factors must be carefully weighed against the cost of accepting noncompliant COTS products with their associated errant output.

Custom Developed Software

Potentially the most difficult of all desktop Y2K issues are the ones dealing with custom applications software, due to the tremendous variety and quantity of installed products, and the difficulty in assessing custom developed software enterprise-wide. The DOIT assumes that all desktop systems in support of mission critical business functions are already being addressed through the *California 2000 Program Guide*, as issued on November 7, 1996. Custom desktop applications supporting necessary business systems should be remediated through an approach similar to that presented in the *California 2000 Program Guide* for mission critical systems.

Critical Success Factors

Several factors are considered critical to the successful remediation of Y2K-impacted desktop systems that support necessary business processes. These critical success factors follow:

1) ***Identify key business areas, ranked by risk to the business. Evaluate the impact of desktop hardware, operating system, and applications software failures for these key areas.*** The proper categorization and classification of risks will force a focus on systems that support necessary business processes. Without a proper risk assessment, resources and time may be wasted on remedying systems that support less than important business functions.

2) ***Prioritize your inventory efforts, so as not to waste time and resources on systems that are ancillary to the necessary business processes of concern.*** Conduct a prioritized inventory based upon the decisions reached in the risk assessment phase. Conducting the inventory of all hardware and software may be desirable, but limited resources may force a prioritization of this effort. Prioritize the inventory against necessary business functions before proceeding to the remediation phase.

3) ***Determine not only the specific problem, but also the most expeditious and cost effective solution to that problem.*** Determine the specific problems of each affected system and prioritize remedies on the basis of necessity to the organization. Without a specific determination of the problem, a specific solution cannot be found.

4) ***Select and employ an appropriate set of automated tools. This will provide great payback in terms of remediation as well as in management of the process.*** Use software tools wherever and whenever possible to capitalize on limited personnel resources and remediation time.

Reminders of these factors are placed throughout applicable sections of the document.

SECTION 2: PROGRAM TIMELINE AND REPORTING REQUIREMENTS

All mission critical systems were subject to reporting requirements set forth in the *California 2000 Program Guide*. The following timeline pertains to desktop systems supporting necessary business functions. Figure 2.1 provides the *California Year 2000 Desktop Systems Program Guide* timeline and major milestones through June of 1999.

Beginning in July 1998, every department will be expected to report its desktop Y2K status to the DOIT on a monthly basis.

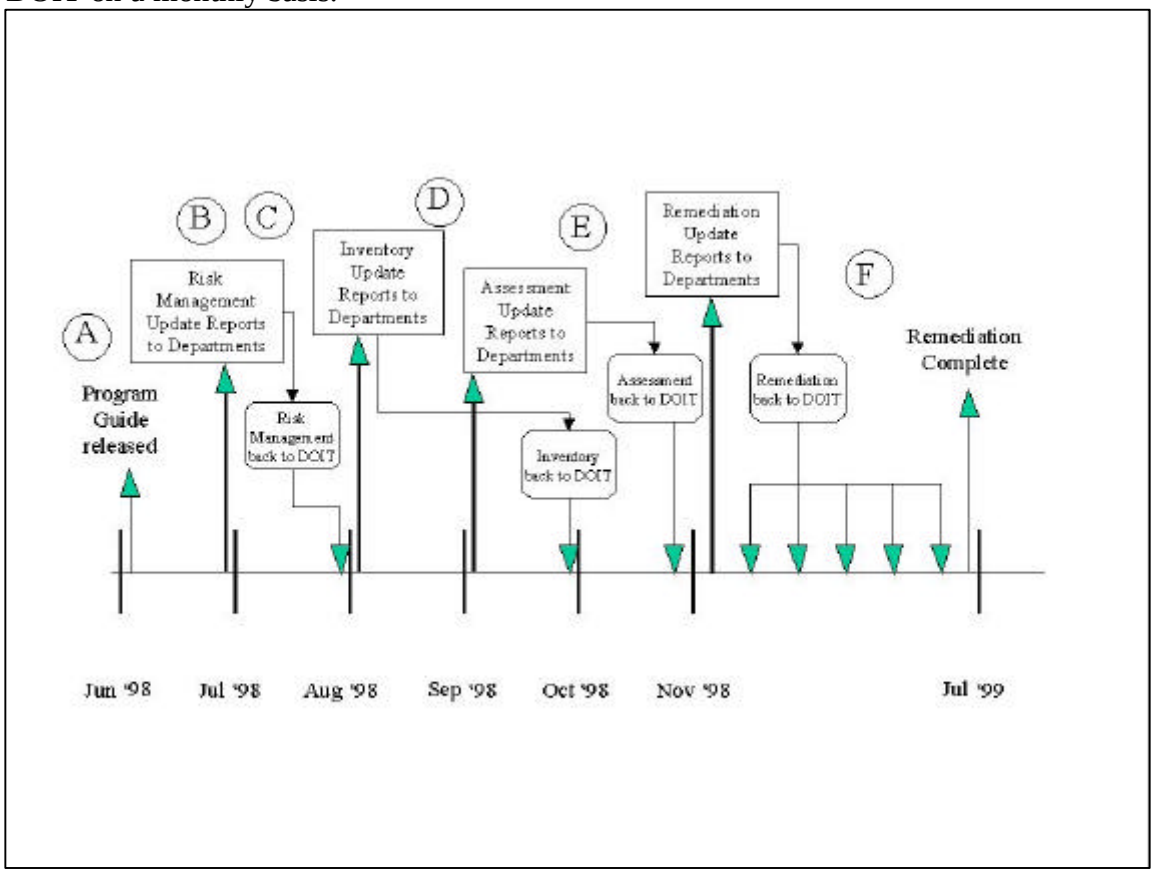

Figure 2.1 - California 2000 Desktop System Program Timeline

The following is a brief description of the California 2000 Desktop Program major milestones and reporting requirements illustrated in Figure 2.1. The timeline sets forth specific due dates for initiation and conclusion of various stages of the process, with the recognition that phases should overlap or be concurrent. Even though certain information must be reported by the date indicated, some departments will be ahead of schedule and should report whatever information is available at the time. Organizations should consider initiating the next phase prior to the full completion of the preceding phase, so that the timeframe for remediation can be compressed as much as possible.

A) **Program Guide -** In June 1998, the *California Year 2000 Desktop Systems Program Guide* is distributed to Chief Information Officers and Department Directors. The purpose of the *California Year 2000 Desktop Systems Program Guide* is to set forth a methodology for a more specific focus on desktop computing environments.

B) **Monthly Update Reports –** Beginning in July of 1998, additions to the existing DOIT Year 2000 Monthly Update Report will be distributed for departments to report updates on their desktop Y2K plans. The supplemental reports will be issued in stages associated with the phases of the effort. Each successive monthly report will include the reporting worksheets from the previous months, allowing for updates and corrections. Monthly update reports for desktop systems will request information pertinent to the status of desktop hardware, applications software, and operating systems that support necessary business processes. Completed reports will be used by the DOIT to monitor departmental desktop Y2K efforts throughout the state, and to report departments' progress to the Administration and to the Legislature.

The first such update report will be issued in July 1998 for risk management, and will elicit a preliminary count of desktop systems supporting necessary business processes. The risk management update report will present a means for classifying the number of high, medium, and low risk desktop-based systems within an organization, but will only request a reporting of the total count of those systems.

The second monthly update report, to be released in August 1998, will request prioritized inventory information for desktop systems. This desktop update report will request counts of servers, workstations, COTS products, custom-developed application software, and operating systems that support necessary business processes. This update report will also request information on whether an automated tool set(s) was used during the inventory phase, and if so, the name of the tool(s).

The third update report, to be released in September 1998, will request desktop assessment results. The total number of desktop systems (servers, workstations, COTS products, custom developed application software, and operating systems) requiring remediation will be requested. Corresponding to the inventory phase, the question of automated assessment tool use will be posed.

The monthly update report to be issued in October 1998 will request identification of plans for dealing with desktop Y2K issues. This final form of the update report will be used to report the number of remediated desktop systems for each remediation path (remediate/replace/retire).

C) **Risk Management** – Risk management activities should be completed by the end of July 1998. Departments should have identified systems supporting necessary business processes, and categorized and classified those risks.

D) **Inventory & Prioritization** - Departmental inventory activities directed toward prioritized business needs should begin as soon as possible, but certainly no later than August 1998. These inventory activities should be completed by the end of September 1998.

E) **Assessment** – The assessment of problems associated with inventoried and prioritized items should commence as soon as practical, but certainly no later than October 1, 1998. Problem assessment should be completed and remediation decisions reached no later than the end of November 1998. Again, recognize that phases within this process are not sequential, so that assessment of one system can be done concurrently with the remediation of another system.

F) **Remediation, Testing & Contingency Planning –** Departments should initiate remediation efforts no later than November 1, 1998. The remediation phase includes testing and verification of the compliance of the impacted hardware/software. By June 30, 1999, all departments should have completed their desktop Y2K remediation efforts. Contingency plans should be drafted as soon as possible, so that operational and procedural alternatives can be prepared. If applicable, time must be scheduled for authorization, procurement, and installation of contingency mechanisms.

SECTION 3: DESKTOP PROGRAM GUIDE METHODOLOGY

This Program Guide presents a means for managing the myriad potential problems associated with the Y2K problem on the desktop. The desktop Y2K problems, whether hardware or software related, can be addressed through the use of this common methodology, which consists of the following phases:

PHASE 1: Risk Management
PHASE 2: Inventory & Prioritization
PHASE 3: Assessment
PHASE 4: Remediation & Testing
PHASE 5: Contingency Planning

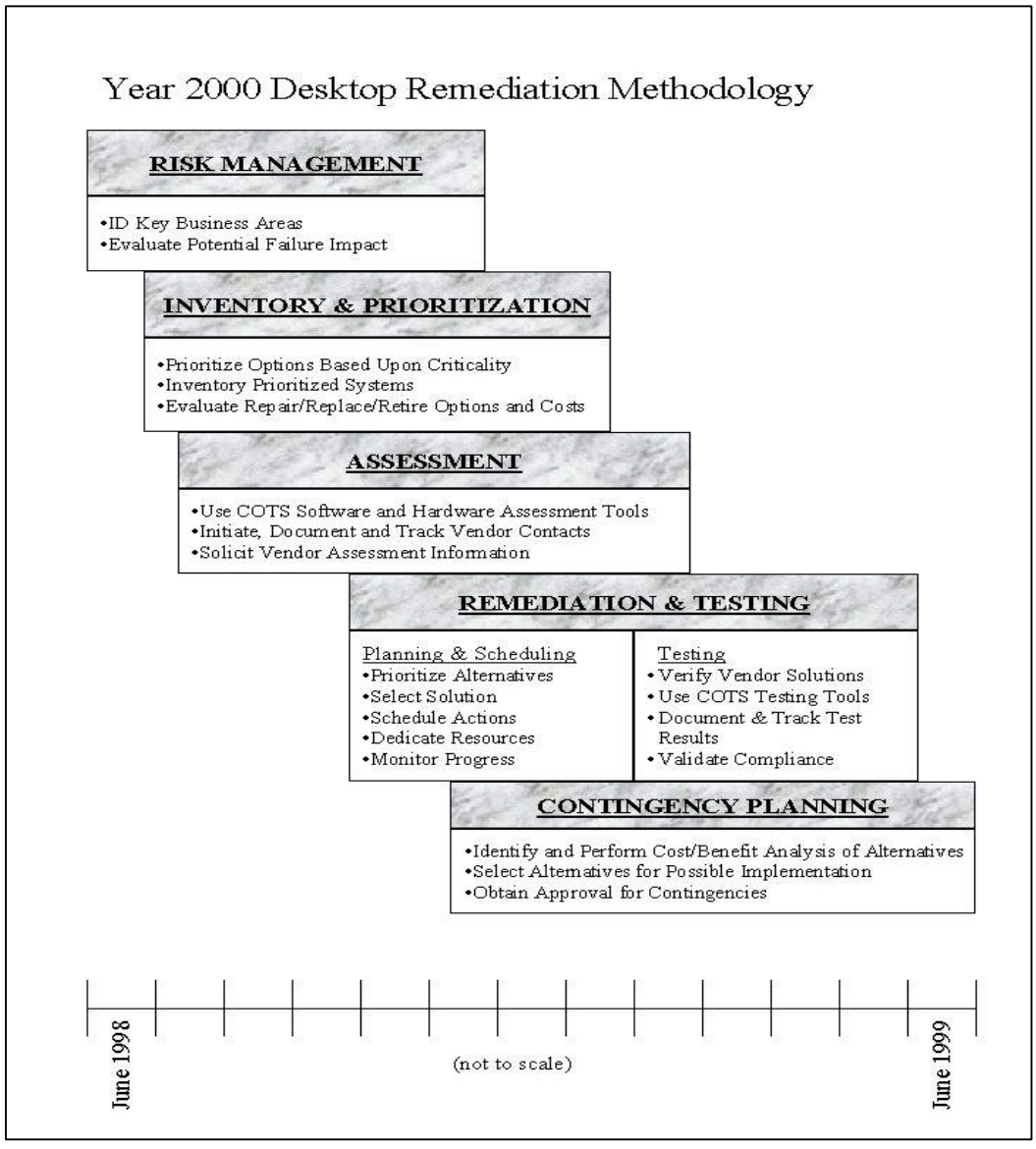

Figure 3.1 - Year 2000 Desktop Remediation Methodology

Figure 3.1 indicates the overall approach that can be taken to remediate the desktop Y2K problem. Please keep in mind that all of these phases may not be necessary for your particular circumstances, nor are these phases totally sequential in nature. This figure merely presents a visual means of representing the desktop Y2K methodology.

PHASE 1: Risk Management

Risk management is the first and most critical stage in solving the Y2K problem on the desktop. Risks to necessary business processes must be both categorized and classified before they can be properly assessed. The risk management process consists of the following five phases:

1. Categorization of Potential Risk Areas
2. Risk Classification
3. Risk Prioritization
4. Risk Management Plan
5. Identification of Strategic Participants

The phases are designed to ensure that risks have been properly identified, categorized, classified, and prioritized so that the next phase in the remediation process (inventory) can proceed accordingly. A more detailed discussion of risk management, along with sample worksheets, is included in Appendix A. The risk management steps are not entirely sequential; for example, some of the strategic participants identified in Section 1.5 may be employed throughout all phases. Each of the steps is described in greater detail below.

> ***CRITICAL SUCCESS FACTOR*: *Identify key business areas, ranked by risk to the business. Evaluate the impact of desktop hardware, operating system, and application software failures for these key areas.***

1.1 Categorization of Potential Business Risk Areas

Business functions that support necessary services, whether external or internal to the organization, must be examined as to their risk of Y2K-related failure. Critical and necessary business functions can be viewed as pertaining to the sustenance of an organization's core missions, programs, or support services. The DOIT has identified five categories within which each necessary business system must be classified. These include:

- Category 1 - **Health and Safety**: where the loss or degradation of these systems could jeopardize the health and safety of California State employees or the public, or the safety of State property or private property.
- Category 2 - **Environmental Impact**: where the loss or degradation of these systems could negatively impact the environment within the State of California.
- Category 3 - **Operational Impact**: where the loss or degradation of these systems could negatively impact the ability of a department to perform its missions.
- Category 4 - **Public Confidence**: where the loss or degradation of these systems could cause the public to lose confidence in the State's government.
- Category 5 – **Other**: systems that are not categorized above.

These categories are mutually exclusive. When systems can be categorized into more than one category, assign the system to the highest applicable category.

Categories 1 and 2 should have been or will be addressed through either the *California 2000 Program Guide* or the *California Year 2000 Embedded System Program Guide*, as appropriate. **For this Desktop Guide, only categories 3 through 5 should apply, because these categories reflect the likely impact areas on *necessary* business systems.**

1.2 Risk Classification

The proper identification and classification of desktop-related risks is imperative to the successful remediation effort. The following elements are provided to help in assessing the risk classification. Risks falling into any of the five categories identified above must be assessed as to their:

- Probability
- Severity
- Impact

Probability refers to the likelihood of an occurrence, usually ranked between 0 (not going to happen) and 1 (going to happen).

Severity equates to the degree of impact on a business function. High impact risks critically affect the budgets, resource requirements, schedules, or product delivery of business processes. Medium severity risks affect business process in a substantial way, but not critically. Low severity risks can be managed within the process, but affect that process nonetheless.

Impact refers to the effects of the risk on its business environment. The impact or consequences of a risk to a business process needs to be considered in relationship to the process' budget, schedule, resource requirements, or business products.

How a department chooses to weigh each of the above elements is subjective. However, an aggregate risk classification should be derived by combining the separate factors for probability, severity, and impact into a single risk classification.

Systems classified with the highest aggregate risk within the five categories must be given top priority for remediation. There are three risk classification levels:

High Risk	One that would cause a necessary business function to fail
Medium Risk	One that would cause a significant impact to the necessary business function
Low Risk	One not expected to impair the overall performance of the necessary business function

Table A.2 in Appendix A is a sample worksheet for risk classification.

1.3 Risk Prioritization

Risk prioritization combines the categorization and classification efforts, and takes those risks deemed as most significant into a structured analytical environment. Tools, such as those listed in Table A.2, the Risk Assessment Worksheet in Appendix A, can be used to define and document the scope of the desktop Y2K problem. Through the use of worksheets such as this, an enterprise-wide view of risks relative to their impact can be documented, prioritized, and weighed. Once a prioritized list has been developed, and senior management has concurred with the problem and authorized a solution, a risk management plan can be developed.

1.4 Risk Management Plan

A risk management plan must be developed in parallel with the remediation implementation plan. A risk management plan consists of three elements:

1. Procedural definition of which activities need to be performed
2. Determination of when activities are to be performed
3. Identification of who will perform the activities

The scheduling of risk management activities parallels closely with contingency planning activities, as described in Section 3, PHASE 5. Refer to Appendix A for a more thorough review of risk management.

1.5 Identify Strategic Participants

As part of developing, adopting, and implementing a risk management plan, actual participants must be identified. Three types of participants are essential for a coherent assessment of risks to necessary business functions:

- Input from **special knowledge experts** within the organization is essential to correctly identify a risk to a business function, as well as to objectively assess that risk's potential impact on the business function.

- **Vendors**, who will play a key role in demonstrating their replacement products' Y2K compliance status, must also be identified.

- A **site coordinator** must be selected and briefed on expectations for each contingency. Details on contingencies and the procedures for these contingencies must be clearly and fully understood by the site coordinator, or else the entire contingency management plan is at risk for that site.

PHASE 2: Inventory & Prioritization

The prioritization of the inventory process is necessary for two reasons: limited time and limited resources. Although the use of automated COTS inventory tools may allow for an almost total roll-up of inventory, the inventory must be prioritized based upon business areas identified as necessary.

> ***CRITICAL SUCCESS FACTOR: Prioritize your inventory efforts, so as not to waste time and resources on systems that are ancillary to the necessary business processes of concern.***

There are two approaches to conducting an inventory: Top-down; and Bottom up.

The fundamental difference between each inventory approach is that one (top-down) identifies the necessary business function first, and then seeks to inventory those items supporting that function, whereas the other (bottom up) identifies all items, then seeks to identify which support necessary business functions.

Ideally, both the top-down business process-driven and the bottom-up inventory-driven assessments should happen simultaneously, thereby maximizing an organization's capture of desktop systems affected by the Y2K problem. However, limits on internal resources, budgets, and time may ultimately preclude a bottom-up, full inventory-based assessment. The generous use of COTS inventory tool sets, such as those listed in Appendix B, should enhance the prospect of a successful capture of the total inventory.

2.1 Top-Down Inventory

The top-down review of necessary business processes will enable an organization to create a list of desktop systems that support necessary business processes. An inventory of those systems, whether conducted manually or via a COTS tool set, will produce an actual hardware and software list of desktop systems requiring assessment.

The inventory may be accomplished through either a manual or an automated effort. For installations where stand-alone desktop units are the norm, COTS inventory tools may be unnecessary. Manual inventory of such systems may be more appropriate, but manual efforts will require the dedication of sufficient personnel to get the job done. A manual inventory should capture the following items:

- Site Identification & Point of Contact
- Desktop Inventory
- Desktop COTS Software Inventory
- Desktop Databases Inventory
- Network Server Inventory
- Server COTS Software Inventory
- Server Databases Inventory
- LAN Inventory
- Inventory of Licensed Software

Appendix C contains samples of inventory worksheets that capture the above items in a structured way.

2.2 Bottom-Up Inventory

In situations where an organization's array of desktop products is tied together via a LAN, the more comprehensive bottom-up approach increases the likelihood that all systems affected by the Y2K problem will be identified. COTS tools that work across a network are very thorough and methodical at logging BIOS manufacture and version data as well as capturing detailed listings of installed software. This comprehensive inventory leads to a broader basis for prioritization.

COTS software tools are geared towards expeditiously gathering and sorting detailed inventories. Use of such tools should be seriously considered because of their time saving benefits.

2.3 Prioritization

Systems that have been prioritized during the risk management phase have already been prioritized for assessment. Changes in business processes may alter the risk classifications associated with those processes, so maintain awareness of internal organizational dynamics.

PHASE 3: Assessment

Following the prioritized identification of necessary business processes and the inventory of items in support of those processes, the next phase deals with the assessment of actual problems within those areas. After a prioritized inventory has taken place, a determination of the solution must be made: whether to replace, repair, retire, or restructure the particular desktop environment currently supporting the identified business process. Often, the most expeditious means of determining the scope of the problem is through the use of commercial automated software tools that can address both hardware and software issues throughout the desktop environment.

> ***CRITICAL SUCCESS FACTOR*: *Determine not only the specific problem, but also the most expeditious and cost effective solution to that problem.***

The overall approach to dealing with assessment of the desktop Y2K problem is the same regardless of the nature of the Y2K problem (hardware, operating system software, or applications software). The assessment process involves the following:

- Assign resources
- Review legal status of maintenance agreements and existing contracts, with related liabilities for both vendors and the State
- Gather list of vendors and compile database of vendor information
- Contact vendors/suppliers
- Establish a tracking system
- Manage the configuration
- Log responses into tracking system
- Identify cost to repair/replace, if vendor's product is noncompliant

Each of these assessment processes is described below.

3.1 Assign resources

An often-overlooked area in the assessment process deals with the assignment of resources. The time and availability of skilled personnel, whether internal or external to the organization, is a critical success factor in the remediation effort of the desktop Y2K problem. The failure to identify or classify a risk because of insufficient or inadequate staffing of the assessment phase could potentially lead to an entire business process being unsupported once the century change takes place.

It is important that the decision on resource allocation be made as early as possible, not only because of the ever reducing quantity of time to complete the remediation process, but also because of the ever increasing demand for qualified external consulting resources, should they be required.

3.2 Review legal status of existing contracts and related liabilities

A separate and ongoing legal review must be undertaken relating to vendor contracts and responsibilities for their products. This legal review will also need to be factored into the remediation/replacement decision-making process. If a vendor's contractual commitment is vague or undefined, it behooves the organization to assume the worst and build such a concern into the remediation/replacement decision-making process.

3.3 Gather list of vendors and compile database of vendor information

The inventory process should have allowed for sufficient capture of vendor identification data to establish a baseline for tracking this information. Using this baseline, identify specific vendor points of contact or information sources (web sites, for example) where compliance data can be captured. Collect this data in a centralized source, such as a spreadsheet or database, for eventual correlation to compliance data.

3.4 Contact vendors/suppliers

The next phase is to obtain compliance information on each product in the inventory. This information is usually obtained directly from the vendors. They can explain what needs to be done to their product, if anything, to make it compliant. Obstacles usually arise, though, when searching for the compliance status of specific products. Although many product manufacturers are releasing Y2K data about their products, the information is available in a wide variety of formats: web pages, databases, word processing documents, form letters, and fax-back forms. Table 3.1 is a partial listing of web page addresses from some of the major manufacturers presenting Y2K information on their products.

3Com	http://www.3com.com/products/yr2000.html
Bay Networks	http://www.baynetworks.com/year2000/
Cisco Systems	http://www.cisco.com/warp/public/752/2000/index.html
Compaq Computer	http://www.compaq.com/year2000/
Hewlett-Packard	http://www.hp.com/gsy/year2000/info.html
IBM	http://www.ibm.com/IBM/year2000/
Lotus Development	http://www/support.lotus.com/home.nsf/welcome/y2k
Microsoft	http://www.microsoft.com/year2000
Novell	http://www.novell.com/p2000

Table 3.1 - Sampling of Manufacturer Y2K Web Sites

What each manufacturer means by Y2K compliance may be inconsistent. The terminology used to document compliance is inconsistent and information is not readily available from many vendors. In addition, a different version of each product may not be

at the same level of compliance due to differing manufactures of BIOS. Be wary, do not accept global statements from vendors, and make a point of being specific in questions asked of the vendors. See Section 7 for further discussion on vendor management issues.

Obtaining compliance information regarding custom software developed in-house will require allocation of internal resources. Refer to Section 6 of this document for specifics regarding assessment of custom application software.

3.5 Establish a tracking system

Logging communications between the vendor and the department will be necessary. Ideally, such logs should be posted into a management tracking system that would enable the department project manager to further assess information towards reaching a remediation/replacement recommendation. Should a vendor indicate pending compliance, the scheduled date and cost of such an event should be logged and weighed against contingencies and the criticality of the vendor's schedule not being met. Alternatively, should a vendor indicate noncompliance, the documentation of such an event is necessary to establish the revised baseline regarding that product.

3.6 Manage the Configuration

The remediation process should be managed through a thoroughly defined "Configuration Management" (CM) plan. CM in this sense implies dealing both with the traditional area of software version control and also with the concept of management of physical (desktops, servers, peripherals, and LAN devices) and soft (software) assets.

CM consists of methods and tools for systematically managing system configuration throughout development, maintenance, and the remediation life cycle process. Specific to Y2K desktop issues, CM can be used to track the status of:

- Vendor compliance schedules
- Software upgrades
- Motherboard replacements
- Remediation tool use and success status

A CM plan should be created specifically to define the items, methods, tools, and organization required to manage the configuration for the Y2K desktop effort.

CM allows for organized changes to life cycle products being managed. It also provides concurrent access during development, thereby supporting creativity, and it also provides discipline and control to avoid chaos and confusion. CM supports the ability to track, allows for control or scope of subcontract requirements, maintains consistency and integrity of the managed system(s) and ensures the reconstruction of system configurations.

Beyond pure configuration management is the concept of *clean management*. The concept of *clean management* can be viewed as the application of strict segmentation and control over and above normal configuration or asset management. *Clean management* is imperative to the success of a Y2K remediation effort, because of the inherently inter-connected nature of the desktop/client/server environment. Without the application of *clean management* principles, desktops or client systems identified as remediated could again become contaminated through the introduction of corrupted date data. As a rough analogy as to the potential for harm due to unclean configuration management, consider the computer virus and its spread throughout the data processing world. Corrupted data can more readily spread than a virus, because users of the data willingly share and ship that data between systems in support of their day-to-day business functions.

Having defined the concepts and benefits of CM, the next step is to identify and acquire a tool that has the architecture and functionality to effectively address the configuration management requirements described above. In addition to CM functionality, this tool should provide accessibility in a most effective and economical manner and continue to provide CM services beyond the Y2K environment.

3.7 Log responses into tracking system

Once a configuration management tool set has been procured and implemented, it can be used to track and log the progress of each identified target of the remediation process. This tool, when used in conjunction with a project manager's strong project management skills, will enable the desktop Y2K problem to be carried forward to a successful conclusion for all business processes targeted for remediation.

3.8 Identify cost to repair/replace, if vendor's product is noncompliant

An obvious component in the remediation process is the determination whether to repair, upgrade or replace a noncompliant desktop product. Costs schedules beyond sheer purchase must be considered; costs such as installation charges, lost work costs resulting from delayed or interrupted work schedules, and training costs are also valid areas for concern. Each of these costs must be totaled and weighed against the costs of viable alternatives, so that the true best value determination can be made.

PHASE 4: Remediation & Testing

The remediation phase encompasses the following activities: 1) planning and scheduling; 2) the actual remediation; and 3) testing and test verification.

4.1 Make repair/replacement/retirement decision

Before any remediation can proceed, a decision must be reached as to repair or replacement of the product. For example, repair can include motherboard replacement or BIOS upgrades. The repair/replacement/retirement decision hinges upon the timeliness and degree of confidence in a vendor's remediation schedule, the cost of repair or replacement of the item, the budgetary cycle and fiscal constraints, and the criticality of the business function being supported by the item in question. The aggregate of these factors must be considered against other high-risk systems/devices in support of other necessary business functions, so as to prioritize the solution response.

4.2 Obtain management approval to proceed

Once all cost and schedule considerations have been addressed in the problem assessment phase, a set of recommendations for remediation must be presented to management for sign-off and approval. Whether a new procurement is requested, or custom software is to be rewritten, management must understand and approve the recommended direction so that all concerned parties are fully informed of the remaining risks, and the costs and benefits of each alternative. Funding must also be coordinated and appropriated with all respective authorizations.

4.3 Coordinate with vendors; schedule repair/replacement

Schedule remediation/replacement issues with the appropriate vendors, and log all relevant details into the configuration management tool. If the vendor is to repair or upgrade the item, schedule the task. If using a tool set to self-repair, apply the tool(s) against the prioritized inventory list. Prioritize through the high-medium-low ranking to assure that priority business processes reliant upon the highest risk desktop systems are remediated first.

4.4 Identify alternative methodologies for validation/testing

Validation and testing can be performed by one of two means:

1. Employment of specific COTS tool sets, if available;
2. Manual verification of test methods and associated results.

Industry best practices indicate that redundancy in testing is judicious. For systems classified as high risk, consider using a dual validation/testing approach, wherein both automated and manual methods are employed.

When using COTS tools, consider employing two distinct tool sets from different vendors. Should one COTS tool not thoroughly test a product due to idiosyncrasies internal to that tool, the second tool will likely catch the oversight. Although redundant testing may seem wasteful in terms of cost and effort, a higher level of confidence in the results is gained through the process.

Similarly, more than one manual testing method should be employed to ensure that idiosyncrasies in the test plans are identified. Manual testing typically comprises establishment of baseline test data with known results, and comparing this data with that generated by the remediated software.

4.5 Validate all repairs/replacements performed

Intermittent vendor contacts may be expected to continue throughout the project. Detailed documentation and managing vendor compliance/response issues are necessary to shield the State from unnecessary risk, and to ensure a proper level of due diligence. Strong project management and schedule coordination skills must be applied to track and ensure the full and timely remediation/replacement of all targeted systems.

4.6 Define test procedures and criteria (vendor or internal)

The various testing methods must be thoroughly evaluated. Determine the test criteria and processes well in advance of conducting the tests to ensure validation of successful test results. Reviews of the test results may generate additional problem identification, and alternate plans for resolution of those problems.

Test criteria and expected results should be assessed by subject matter experts for application software, and by IT support staff for hardware and operating systems.

4.7 Define/assign responsibilities for testing

Coordinators must be assigned at each site where tests are to be conducted and/or overseen. Staff with appropriate knowledge and awareness, such as the subject matter experts referenced in Section 1.5, should be selected to conduct and/or oversee the testing, whether it is performed by in-house or contract resources. Assigned coordinators must have access to a sufficiently high level of management to provide leverage against non-performing or recalcitrant testers.

4.8 Conduct tests or verify test results

Prior to initiation of the performance tests, careful deliberation must be given to defining the measures of success. Tests must be conducted with success parameters predefined. Monitoring and capture of test results is imperative for a valid assessment of those results.

4.9 Assess results

When testing is completed, careful analysis must be made of the observed and recorded results as measured against the predefined measurement criteria specified in Section 4.6.

Significant deviations between the actual and expected results must be documented and accounted for.

4.10 Identify problem areas and track resolution

Problems identified prior to, during, or subsequent to testing must be documented and logged into the configuration management system. Risk management issues must be considered in order to determine the appropriateness of initiating contingencies. Problems of sufficient magnitude must be presented to management to allow for adjustment of pertinent risk factors.

PHASE 5: Contingency Planning

Based on the preceding remediation and testing effort, contingency plans must be developed. Proper contingency planning will aid in:

- Mitigating the likelihood of the risk occurring;
- Minimizing the nature of the risk;
- Providing for contingencies in the event the risk occurs.

The phases requisite to developing a contingency plan are:

- Identify and prioritize situations for which planning is necessary;
- Consider grouping common areas or elements in order to realize economies of scale;
- Consider alternatives for each situation;
- Select the most appropriate action for dealing with the situation, or establish criteria to determine the actions to be taken;
- Divide actions into the following groups:
    a) Those to be taken prior to the event;
    b) Those to be taken if the event occurs;
    c) Those to be taken if the event does not occur.
- Develop contingency procedures;
- Train applicable staff in the use of the contingency procedures.

Contingency planning requires appropriate approval by management. The approval process verifies the validity of contingency plans as developed, maintains a high-level awareness of the problem, and establishes concurrence in how the risk will be addressed and/or mitigated.

As in the risk assessment phase, participants in the contingency planning phase include:

- further **vendor** involvement, because viable contingency planning must include assessment of the compliance of proposed alternatives
- business **subject matter experts** to ascertain the viability of potential alternatives and their respective impacts on the business function
- **site coordinators** to carry out the planned contingencies, should the need arise. These individuals must be fully informed as to the occasions and specific tasks to be instituted in the event of the failure of a necessary business function.

SECTION 4: DESKTOP HARDWARE

The root of the problem in desktop computing hardware is the Basic Input/Output System (BIOS), the software built into each PC that controls the fundamental hardware operations and the Real Time Clock (RTC) chip that actually keeps time just as a digital clock does. Most manufacturers did not code their BIOS with the ability to automatically adjust the incorrect year generated by the real time clock on the first day of the century roll over. Older PC models, such as 386s and 486s, and even some Pentium computers, will have problems unless correctly remediated. Many PC manufacturers have made Y2K compliant versions of their BIOS available.

The BIOS problem, however, is not limited to older PCs. Many desktop and server models released as late as 1997 have a BIOS that will not correct the system date unless updated.

Purchasing new systems to avoid the Y2K problem is not the panacea many thought it would be. For example, Table 4.1 shows the range of Y2K desktop hardware problems.

HARDWARE	DETERMINATION
386 PCs	Replace hard BIOS or replace unit
486 PCs	Undetermined; may have flash[1] BIOS
Pentium / 586	Most have flash BIOS, or not a problem

Table 4.1 - Desktop Computer Hardware Y2K Status

The BIOS of every desktop system, whether it is old or new, should be inspected or verified to be certain of its Y2K compliance.

When following the 5-phase methodology as it relates to desktop hardware, specific issues should be considered. These issues are presented within the respective phase, below.

PHASE 1: Risk Management

Regarding issues affecting desktop hardware, the most critical from a risk perspective are the servers. Should a server report an incorrect date to application software throughout the network, or should date synchronization between it and another server be lost, necessary business functions could suffer. Stand-alone or client desktop computers, although reliant upon the same BIOS function to send the date to the operating system, do not individually have the same level of impact to business function as do servers.

Hubs and network interface cards **do not appear** to have a Y2K problem. To date, there have been no reports of, nor have vendors indicated any problems with, these hardware types.

[1] Flash BIOS compatible computers are those capable of receiving updated BIOS routines without physical replacement.

PHASE 2: Inventory & Prioritization

Given their critical function, LAN servers are clearly a priority for inventory. Desktops, whether client or stand-alone, must also be inventoried, but only when in support of necessary business functions.

Worksheets in Appendix C will assist in the inventory of servers and desktop units.

PHASE 3: Assessment

Two parallel approaches to assessment should be considered. First, obtain vendor compliance information, by written statement or through published compliance lists. Second, obtain actual Y2K compliance data from testing, either through COTS tools or through tests developed to address the specifics of the environment.

The first approach does not guarantee compliance, even if a vendor certifies that its hardware will not cause date-related problems. The second approach offers several alternatives for obtaining Y2K compliance data. COTS assessment tools may be used to verify compliance. The use of COTS assessment tools is highly recommended. Nevertheless, it is also recommended to adopt two such tools and employ them in parallel, thereby increasing the degree of confidence in the results. Also, one may research published assessment results, often provided by vendors themselves.

The assessment phase is applied somewhat differently for client or stand-alone desktops/laptops than for network servers. Each is discussed below.

Client or Stand-alone Desktops/Laptops

Client-type desktop and portable computing devices can be readily isolated from the network to allow for discrete testing and remediation of hardware-related issues. A client machine can be brought off-line from a network for testing with little impact to the overall environment.

If there are only a few PCs potentially affected within an organization, the following simple test can be performed, requiring no special software.

Caution:	***If there is any time-limited software on the PC, the test is not recommended. Advancing the date could trigger the software expiration date and render it useless. To be absolutely safe, perform a complete backup of your computer before the test.***

Simple Test

1. Back up the computer system
2. Change the time and date of your PC to 11:55 p.m., Dec. 31, 1999
3. Turn the computer off for 10 minutes
4. Turn the computer on and check the date and time
5. Once testing is complete, reset to correct date and time, shut down the computer, and power up

Noncompliant systems will show an incorrect date, such as one in 1980 or 1900. A similar test may be performed relative to the leap year by changing the date to February 28, 2000. Some computers won't recognize that 2000 is a leap year and will skip over February 29. Remember to reset the computer back to today's date after performing this test.

COTS tools, such as those referenced in Appendix B, can check for BIOS compliance by checking the BIOS version against a list of known products and their respective compliance/noncompliance. Similarly, both tool driven and manual tests can be used to balance against the manufacturer's statements regarding Y2K compliance of their product.

Network Servers

Servers are devices that typically house application software and database data that are shared by client desktop systems. Servers can be viewed as supporting a variety of functions: LANs, Internet access, and common printing/fax facilities. The key position that servers play in relation to the clients they serve virtually assures impact to the whole environment should a problem develop. Redundancy within a server environment, while normally allowing for continuity of operation, does not guarantee functionality in the event of a Y2K-related failure across multiple servers.

The technique used to test network servers for Y2K compliance is similar to that used to test personal desktop or client computers. The test of the system clock on network servers involves a few simple steps to set the system clock forward and evaluate the effects. As with personal computers, conducting this test requires shutting down the server so that the date change will take effect. Obviously, shutting down the server affects all network users attached to that server and dictates that the test is carefully scheduled well in advance. As with any computer test, **the server should be fully backed up prior to initiating this procedure**. The steps in this process are:

1. Ensure that a complete backup has been performed on the server.
2. Check that all users have logged off the server.
3. Set the system clock to a date and time just minutes prior to January 1, 2000 such as December 31, 1999; 11:55 PM.

4. Shut the computer down for 10 minutes to allow the date change to take effect
5. Bring the server back up.
6. Verify that the server re-started properly.
7. Check the date and time on the server.
8. From a workstation, log on to the server to verify that users can access the server.
9. Once testing is complete, remember to reset to correct date and time, bring the server back down, and then back up.

The purpose of this test is to determine if the server in question can accurately handle the millennium rollover. A similar test should be used to assess leap year recognition. The network operating system running on the server must be tested separately.

Unlike personal computers which are routinely shut down and/or re-booted, servers typically operate for long periods of time without interruption of operation. When network server operations are commenced, some settings, services, and software may require manual configuration and/or initiation in order for the network to function properly. These manual interventions are in addition to those that automatically load. Examples of these settings, services, and software are: device drivers, network system settings, protocol and security services, and resident applications such as automated backup utilities. Because of the complex nature of the server environment, it is highly recommended that the system administrator responsible for configuration and maintenance of the network server be present when the rollover test is conducted. Additionally, available server configuration documentation should be consulted. Finally, double check both of these sources by accessing the server console and issuing the necessary commands to display a list of drivers, services, and software loaded on the server prior to testing. Compare this list to the setting in any configuration files which are automatically executed at boot-up to ascertain any manual intervention that might be necessary.

Another issue to consider with regard to network servers is the date and time synchronization that occurs between servers on multi-segment LANs running certain network operating systems. This is especially important if servers on the multi-segment LAN are of different manufacturers. After each individual server has been evaluated for Y2K compliance, all of the servers on the LAN should be brought up and allowed to operate for a few minutes with the system clocks still set to a date time beyond January 1, 2000. During this time, using certified compliant workstations attached to each segment of the LAN, log on to the network and verify that each server on the LAN has the correct date and time.

PHASE 4: Remediation & Testing

Remediation strategy should follow the lowest cost/most expedient path to solution:

1. Flash BIOS upgrade
2. Terminate and Stay Resident (TSR) patches
3. Daughterboard insertion
4. System replacement

Flash BIOS replacement deals with updating the BIOS software settings externally, without chip replacement. Only certain BIOSs are equipped to handle this type of fix.

TSR patches can be used to mask the date problem by intercepting errant dates between the operating system and resident applications, or between applications themselves. This remedy places a high degree of reliance on the TSR software.

Daughterboard insertion deals with placing specialized computer boards into a noncompliant desktop, with the daughterboard taking over the date-handling function from the motherboard. This approach can be quite cost effective, but requires technician installation and testing time beyond some of the other options.

System replacement may be the surest remediation method, but is also the most costly. Remember to insist on Y2K compliance details before purchasing any new system, because new systems could still contain an older, noncompliant BIOS.

The same testing regimen used for the assessment phase can be used for verification of the remedy.

PHASE 5: Contingency Planning

Contingency considerations in the desktop computing hardware area include:

- Back-up network servers;
- Leasing of desktops;
- Redirection of internal resources (i.e., use compliant hardware where necessary, moving noncompliant hardware to non-essential support positions).

SECTION 5: OPERATING SYSTEMS

Most major operating systems were coded to support four-digit years; others can be changed with a patch. This ability is useless if a noncompliant BIOS transfers an incorrect year to the operating system's date stamp. Each time the operating system or network operating system transfers an incorrect year to an application that requests it, any number of errors can occur. Users may experience mishaps ranging from calculation and sorting errors to invalid logic. Some of the errors would be instantly obvious, but others could pass by unnoticed until entire systems are corrupted.

Desktop Operating Systems

The most prevalent desktop operating systems, MS-DOS, Windows 3.1, and Windows 95, are known to have BIOS recognition problems. MS-DOS will interpret 2000 as an invalid date and store 1-1-1980 as the system date, because this is the earliest it can recognize. Microsoft Windows 3.1 and Windows 95 will also interpret the year 2000 incorrectly, but patches are available from the vendor.

Network Operating Systems

Some operating systems, such as Microsoft Windows NT 4.0, keep a date stamp and have the ability to correct erroneous dates from the BIOS. However, other major operating systems do not have this ability, including Novell NetWare 3.12, and IntraNetWare 4.11. UNIX versions do not appear to have the same problem as their traditional desktop cousins, and so are not impacted by Y2K date problems.

Table 5.1 identifies the range of Y2K problems within common operating system software. For those operating systems not listed in Table 5.1, refer to the vendor for a compliance determination.

OPERATING SYSTEM SOFTWARE	DETERMINATION
MS-DOS Version 5.2 – 6.0	Known problems. Manual intervention required.
Windows 3.1	Known problems; patches available.
Windows for WorkGroups	Vendor Y2K compliance assertion.
Windows 95	Known problems; patches available.
Windows 98	Compliant
MAC OS	Compliant
OS/2 Warp 4	Compliant
Windows NT 4	Compliant
Microsoft LAN Manager 2.1	Unknown
Novell NetWare 386	Noncompliant
Novell NetWare 4.1	Vendor claims patch corrects known problems

Table 5.1 - Operating System Y2K Status

PHASE 1: Risk Management

Network operating systems pose the greatest potential risk to necessary business processes. Desktop operating systems, although much more prevalent than their network counterparts, are typically standardized with few versions resident within an organization. The risk associated with a desktop/OS failure in date provision to applications can affect important business activities.

PHASE 2: Inventory & Prioritization

> *All NOSs should be inventoried because of their centralized position within the business environment. Determining the necessity of a full desktop OS inventory should be based upon the risk management results.*

Appendix C provides several example worksheets for manual inventory data collection. Alternatively, COTS inventory products, listed in Appendix B, will provide a ready source of detail on the OSs and NOSs within the target environment.

PHASE 3: Assessment

NOS

Use the same approach as outlined for Assessing Network Servers in Section 4. Care must be taken, however, in coordinating with all users, including off-hour users such as system administrators, in isolating the network for assessment. The order of shutdown and boot-up should be carefully considered, in the event that noncompliant hardware infects clean NOSs with errant dates.

Desktop OS

Employ the same methods and approach as used for Desktop Computer Hardware in Section 4.

PHASE 4: Remediation & Testing

Should remediation be necessary, considerations should include:

- Verification of replacement/upgrade OS compliance/noncompliance from vendor
- Purchase of Y2K compliant OSs
- Installation of purchased OSs
- Re-testing of installed OSs

PHASE 5: Contingency Planning

Consider fallbacks to COTS and custom applications affected by noncompliant-induced error. Each of these systems must be considered on a case-by-case basis.

SECTION 6: APPLICATION SOFTWARE

Application software is divided into two areas: COTS Software and Custom Application Software. Each is addressed below.

COTS Software

Commercial application software should be verified against its manufacturer's statement of compliance. Additionally, a number of COTS testing tools are available for assistance, especially in the spreadsheet arena. A sampling of COTS software products and their Y2K compliance is presented in Table 6.1.

COTS SOFTWARE	DETERMINATION
MS Access 95	Up to 1999
MS Access 97	Fixed window through 2029
Visual FoxPro 5	Variable window, code dependent
MS Excel Version 2.x – current	Fixed window through 2029
MS Project Version 4.0 – 7.0	Versions < 4.0 are noncompliant. Current release is okay.
MS Word Version 5.0 – 7.0x	Some minor problems have been reported.
MS Exchange	Vendor Y2K compliance assertion.
123	Up to 1999
dBASE 5.5	Up to 1999
Novell GroupWise 4.1	Compliant

Table 6.1 - Common COTS Software Y2K Status

Custom Application Software

One of the largest unexplored Y2K areas relates to custom-developed software residing on the desktop. Whether a custom application was developed in-house or purchased as part of a vendor's service, the identity of such systems, and more importantly, their potential reliance upon an erroneous or deficient date calculation, are areas most difficult to ascertain. Even when such an application has been identified as supporting a necessary business function, documentation may not exist, or corporate knowledge within the organization as to the internal mechanics of the application may be lacking.

This software may have been developed using a variety of languages such dBASE, Clipper, FoxPro, Visual Basic, PowerBuilder, C++, or Oracle PL/SQL and Forms. These systems face the same Y2K date issues that affect many mainframe systems. The level of impact of noncompliance depends upon how the language handles dates internally, and how the programmers chose to store, represent, and manipulate dates within their programs. In general, custom-developed applications will present a more serious problem to an organization than off-the-shelf applications because of these complexities.

Most desktop custom applications are meant to support specific business units within an agency and therefore lack the centralized management of mainframe applications. In this era of client/server software and integrated systems, it is not unusual for an agency to have a custom

developed asset management system developed in one of the above mentioned languages that must exchange data with a commercial off-the-shelf accounting package. In cases such as these, one noncompliant application can render many systems useless. This makes it difficult to document what type of applications exist and to locate exactly where each application is vulnerable.

In addition, upgrading a custom application is not as straightforward as purchasing licenses for a new version. A software engineer with expertise in the language of each specific application needs to inspect every affected line of code to be sure it can correctly process the Y2K. Making custom-designed applications compliant will be very costly in terms of both time and money.

Consider one example: Data from a spreadsheet is passed to another spreadsheet of a different version. The second spreadsheet in turn passes calculated data to yet another spreadsheet of another version. Finally, the manipulated data is uploaded to a mainframe computer, where calculations are performed in support of a necessary business function. Given that various versions of spreadsheets may not treat date data in a consistent manner, a real potential exists for corrupt data from the client/server environment infiltrating the previously cleansed mainframe environment.

PHASE 1: Risk Management

Of the two types of application software, custom-developed applications software poses a greater risk to a business function only because of its uniqueness. For this reason as well, it is much more difficult to remedy a customized solution than a COTS one, either by repair or replacement.

The management of risks tied to custom application software is the same as for legacy information technology applications. Prioritization of necessary business processes and the related list of desktop systems in support of those processes are crucial to success.

PHASE 2: Inventory & Prioritization

Inventory must be driven by the risk management activity. Because of the uniqueness of custom developed application software, an exhaustive analysis must be performed.

PHASE 3: Assessment

Steps necessary for determining a product's compliance within the assessment phase are the same as for compliance validation in the remediation phase. Addressed first are COTS software issues, followed by a discussion of issues pertaining to custom application software.

COTS Software

Determination of the compliance or noncompliance of these products is relatively straightforward:

- Review compliance databases to ascertain identification of known problems.
- Contact the vendor for compliance determination.

- Verify compliance by vendor provided, vendor demonstrated, vendor suggested and/or third-party tests.

If product compliance information is unavailable, consider either generating and conducting your own tests, replacing the product, or accepting the consequences of the failure of the product. Should remediation be necessary, consider an upgrade to the existing product, or purchase a compliant product. Make certain to include resource estimates for converting resident data to the new application.

Custom-Developed Software

To identify the potential exposures caused by using 2-digit-year representations of dates within custom-developed software, a thorough analysis must be conducted to locate references to all date-related data. Remediation of custom developed software should follow a similar methodology to that offered in the *California 2000 Program Guide*.

Consider using the following approach:

1. Locate references
2. Determine the impact of 2-digit-year data fields
3. Investigate how other software entities use the data

Locate References

Following are some recommended manual techniques for locating noncompliant date references.

First, review program information for date references to include, for example, date variables, date functions or routines, and character strings. Character strings might include the following in either your code or its comments:

- ASOF
- AS-OF
- BEG
- BEGIN
- BGN
- CCYY
- CURR
- CURRENT
- CYYDDD
- CYYDDMM
- CYYMMDD
- DA
- DAT
- DATE
- DAY
- DD
- DDDYY
- DDMMYY
- DIFFDATE
- DOB
- DOH
- DT
- DTE
- END
- EXP
- EXPIRE
- JULIAN
- MDY
- MMDDYY
- MMM
- MMYY
- MO
- MON
- MONTH
- START
- TERM
- THISDATE
- TIME
- TIMEDATE
- TIMESTAMP
- TIME-STAMP
- TOD
- T-O-D
- WEEK
- WEEKDAY
- YEAR
- YMD
- YR
- YY
- YYDDD
- YYMMDD

These character strings can be found in any of the following source files:

- Data entry forms, screen display formats, report formats
- Definitions of data fields, records, structures, files, and databases
- Source code, computer program listings, cross-reference reports
- Command languages, such as MS-DOS batch language
- Data indexes and catalogs, table sizes
- Data dictionaries
- Date/time service routines
- Sort routines

Second, use a test system. Install an isolated, non-production system with a duplicated image of your system and application software. It is important that the test environment be completely segregated from the production system to guarantee avoidance of conflicts and contamination of the production system.

Determine the Impact of 2-Digit-Year Data Fields

Once you have located date-related data fields by one or more of the above approaches, the next step is to prioritize or classify the use or reference of those fields into one of the following categories:

1. Low Impact
   - The program uses a 4-digit-year representation in all occurrences.
   - The program uses a 2-digit-year representation within a program, but does not have any internal exposures, nor does it externalize the 2-digit year in any way.
   - The program uses a 2-digit-year representation within a program, but does not have internal exposures. The 2-digit year is externalized, but cannot be referenced (for example, for display-only) by any other program.
2. High Impact
   - The program uses a 2-digit-year representation within a program. It does not have internal exposures, but the 2-digit year is externalized and could be referenced by another program.
   - The program uses a 2-digit-year representation and has internal exposures.

Investigate How Other Software Entities Use The Data

It is important to investigate the ways data is shared among software entities. The greater the degree and scope of data sharing, the more global is the task and the more critical is the need to prevent the further propagation of and data “contamination” by 2-digit-year data.

PHASE 4: Remediation & Testing

Remediation of COTS application software is as straight-forward as its assessment:

- Apply a software patch, if available and appropriate
- Upgrade the software
- Replace the software and migrate the current data into the new environment

Remediation of custom-developed software should follow the guidelines put forth in the *California 2000 Program Guide*.

Testing of remediated application software, whether COTS or custom-developed, should follow the same guidelines identified in the PHASE 3 discussion, above.

PHASE 5: Contingency Planning

Contingency planning for noncompliant applications software, be it COTS or custom-developed, presents a particular challenge.

COTS software replacement should be a straightforward issue of procurement and installation. Personnel resource issues, computer hardware suitability to newer software, and installation scheduling issues are all critical to the successful remediation of noncompliant COTS products. Remember to consider any requirements for data conversion due to changes in COTS software.

Custom-developed applications software poses the greatest challenge of all desktop issues because of its uniqueness. Time is the most critical element in developing new, Y2K compliant applications, modifying those already in use, or procuring COTS products to replace the custom software. This last option of procuring a COTS product to replace a custom application may require a significant adjustment to the current mode of business operations in order for it to be successfully implemented.

SECTION 7: VENDOR MANAGEMENT

How vendors are managed specific to communications and acts is crucial to the successful remediation of the desktop. Vendor management issues cross the breadth of the methodology, from risk assessment issues through remediation testing. Vendor involvement must be managed in such a way as to elicit cooperative and informative responses in an attempt to resolve all problems and avert possible legal action. Precisely how to approach vendors to maximize cooperation is the subject of this section.

The whole issue of legal ramifications, for both the State and also for the vendor community, is an area of intense concern. *These legal issues are not in the purview of this Program Guide*. The overall question as to the State's liability, and its link to the liability of the applicable vendors, is also beyond the scope of this document. As a general rule, however, the legal staff of each organization should review the organization's exposure, and establish a process to ensure "due diligence."

Addressed below are four principal areas of concern regarding vendor communications:

- Identification of responsible vendor contacts
- Reliability and stability of vendor information
- Communication methods
- Compliance data capture

7.1 Identification of responsible vendor contacts

Vendor contact information varies widely from company to company. Some firms identify specific parties to contact within their web sites. More often, however, information and not specific individuals are referenced. Repeated telephone calls or electronic mail (E-mail) messages may elicit feedback from an identifiable party, but the responding party is often a clerk or technician and not at a sufficiently high level of responsibility within the organization. Identifying a responsible vendor contact may be difficult, due both to the degree of automation within our present society and also due to the legal barriers already being raised by vendors in an effort to shield their liabilities.

7.2 Reliability and stability of vendor information

Determining the reliability of compliance information obtained from a vendor is a complex issue. Merely establishing that a vendor issued a product compliance notice at a certain point in time may not be sufficient to ensure that product's actual compliance. The same questions need to be raised for published vendor test results. Due diligence and contingency planning issues should be brought to the forefront of consideration at this point.

The question of the stability of vendor supplied data is also a concern. Vendors can and do alter product compliance information, especially through electronic-based media (web

sites and E-mail). A periodic and ongoing review of vendor supplied compliance information should be inherent in any remediation process.

7.3 Communication Methods

To date, the most successful vendor product compliance gathering efforts have been conducted informally. Informal in this case relates not so much as to how the data was gathered, but rather relates to the approach employed in dealing with the vendor contact.

The concept of informal communications in this regard relies upon non-threatening communications, as viewed by the vendor contact. The tone as well as the message of the communication is of paramount importance in eliciting an informative response from the vendor contact.

Should an informal approach be insufficient, more formal communications must be employed. This approach consists of official documentation, wherein compliance information is requested by the State organization, rather than from an individual within that organization. Elevating the communication to this level has been an increasing requirement, because of vague, insufficient, or null responses from vendors. Consult with your organization's legal staff regarding the due diligence aspects of formal communication and documentation.

Both informal and formal communications should be fully documented, including such items as date and time of call, person contacted, person doing the contacting, and outcome of discussion. A sample vendor data log worksheet is shown in Table 7.1, below.

7.4 Compliance Data Capture

Product compliance information is at the heart of communications. Knowing what to ask, as well as properly and accurately recording the results of the communication, is the key to meaningful compliance data capture. At a minimum, the information that should be captured and recorded for each communication is indicated in Table 7.1, below.

Product Identifier	Name	Manufacturer Prod. No.
Product Manufacturer	Name	
Web-site	Address	
Fax	City, State, Zipcode	
Contact Person	Contact Phone	Contact E-mail Address
Alt. Contact Person	Alt. Contact Phone	Alt. Contact E-mail Address
Date	Time	Dept. Contact Name
Results/comments		

Table 7.1 - Vendor Data Log Worksheet

The top portion of the worksheet contains general information common to an issue. These items are not likely to change from communication to communication, with the exception of personal contact specifics. The bottom portion of the worksheet is for capture of the nature, course, and results of the communication.

SECTION 8: LESSONS LEARNED

The DOIT has begun collecting lessons learned from individual organizations within State government relative to their Y2K Desktop issues. A sample lessons learned, from CalTrans, is described below.

8.1 The CalTrans Experience

Below are lessons learned from the Department of Transportation's efforts to date.

Scope of the Effort

CalTrans is implementing a network asset management program for the purpose of identifying the Y2K problems in both hardware and software throughout its statewide network. Their responsibility is to ensure compliance for desktops, laptops, and client/server environments statewide.

During the course of the project, CalTrans audited 5,636 desktop computers in its Novell tree. CalTrans chose to install and use LAN Supervision's Enterprise Inventory Auditor (EIA) tool as a means of enhancing and expediting their inventory and assessment phases. This tool provided CalTrans with a total inventory count of 684 software packages with 95,197 varieties of these components throughout the entire state system. This total count included desktop hardware, OSs, NOSs, COTS, and custom applications.

Initially using a database provided by the State of Washington as a base-line, CalTrans found that 5 percent of the installed packages state-wide (34 of 684) were non-Y2K compliant and another 5 percent of the packages were compliant, leaving 90 percent of the packages in undetermined status. The use of the EIA product has further refined CalTrans staff's assessment to conclude that only 2 percent of the instances are non-Y2K compliant, and over 23 percent of the instances are compliant, leaving 75 percent of the instances in undetermined status. Therefore, the EIA tool has thus far enabled CalTrans to reduce the undetermined status from 90 percent to 75 percent, yielding an immediate staff hour reduction return-on-investment.

Management Challenges

The greatest hurdle that CalTrans staff encountered was not a technical one, but rather one of ***awareness*** and ***cooperation***. These issues surfaced primarily because of the nature of operation of the inventory/asset management software, which required installation of a login script on every server machine. These issues came on several fronts:

- Many employees felt a personal resentment at having an automated login script run against "their PC" every day. Some individuals were suspicious of the thought that "big brother" was watching their desktop or laptop computer as to its software and hardware base, and thought that the software may actually be examining more than advertised.

- The newly installed EIA software became a 'lightening rod" for complaints unrelated to the product or its use. Headquarters technical staff was required to work many hours on resolving technical issues unrelated to the EIA product or its daily operations in answer to customer complaints.
- District technical support staff tended to override the asset management system settings in response to their constituents' complaints, because staff had not been properly acquainted with the management systems requirements and associated benefits. Configuration settings within Windows .INI files, for example, were changed, resulting in the EIA software's inability to perform its function.

As a direct result of these issues***, internal support staffing requirements were underestimated***. This underestimation caused a strain on the staff assigned, delays in implementation in portions of the network, and ultimately resulted in significant time being spent in overcoming resentment and rumors.

Technical Challenges

As an indirect result of installing the automated daily login, CalTrans discovered a number of systems ***incorrectly configured*** for maximum efficiency. After installation of the EIA software, systems that had been functioning adequately could no longer do so because of the small amount of additional memory required for the automated daily login. CalTrans staff was required to respond to resultant user complaints by altering memory utilization configurations on a case-by-case basis. The staffing loads for this aspect of the effort were not initially recognized, causing additional strain on already limited resources.

Problems relative to the structure of the Novell tree created an opportunity for the improvement of the existing structure, a benefit not anticipated as a result of the Y2K remediation effort. Technical staff must now come to grips with redesign and restructure of the tree, an area where resource loading was not anticipated.

Policy Challenges

CalTrans has uncovered, and not yet fully resolved, ***a number of policy challenges*** pertaining to its implementation of the corporate inventory/asset management system. These issues do not relate to the Y2K remediation effort, but are indicative of the issues being raised throughout the entire Y2K remediation effort:

1. How should CalTrans deal with bootleg software that is uncovered through the inventory process?
2. Are there any limits to inventorying and assessing State-owned software installed on personal desktop and laptop computers used for State work, and if so, what are those limits?
3. What policy statements need to change as a result of possible restructuring or reorganization resulting from this comprehensive enterprise-wide assessment?

Lessons Learned

The two principal issues faced by CalTrans throughout the course of their implementation of the inventory/asset management system were:

1. **Management**: Obtain Recognition/Ownership of the Problem as Soon as Possible
Buy-in by upper management, middle management, line management, and technical support staff is critical to the implementation, maintenance, and success of a Y2K remediation effort. True buy-in and commitment to the program will only come once each of these staffing levels has been informed of their respective benefits under the program.

Upper management needs to understand potential risks and benefits, and to set the stage for commitment by all levels of the organization. The benefits message to upper management should be one of organizational economies of scale through controlled inventory/asset management.

Middle management needs to carry that commitment message down through the organization. The benefit of interest to this level of management is one of enhanced control over limited resources.

Line managers must carry the message through to the staff as a whole. The chief benefit to line managers is the maintenance of and enhancement to daily operations.

Technical support staff, such as PC coordinators and LAN administrators, need to be informed as to their role in the program. Informed support staff, when presented with benefits to their technical areas of responsibility, such as a more efficient Novell tree, will welcome and support the program.

Individual staff members need to recognize the impact of compliance or noncompliance for their desktop. They must clearly understand that the benefits of an enterprise-wide program should transcend the inconveniences to individuals. Finally, the benefits of a correctly functioning workstation after the century change will speak for itself.

The sooner these benefits are demonstrated to the affected parties, the sooner they will cooperate with the entire remediation effort.

2. **Management**: Assess Staffing Resource Availability versus Projections
Projections of resource requirements must take into the account the unexpected. CalTrans encountered difficulties in responding to multiple trouble calls -- some legitimately related to the installation of the EIA system, but some falsely equated with the system. All calls consumed resource time designated for other assignments.

3. **Management**: Determine Travel Costs per Site Visit
The cost of travel to sites as opposed to a distributed installation via network must be examined. Some work sites are not accessible via network connections, so travel costs must be assessed when considering the total cost of remediation.

SECTION 9: GLOSSARY

Term	Description
BIOS	Basic Input Output System
COTS	Commercial-Off-The-Shelf
DOIT	Department of Information Technology
E-mail	Electronic Mail
IT	Information Technology
LAN	Local Area Network
NOS	Network Operating System
OS	Operating System
PC	Personal Computer
TSR	Terminate and Stay Resident
Y2K	Year 2000
WAN	Wide Area Network

APPENDIX A: RISK MANAGEMENT

What is Risk Management?

Risk Management is defined in the State Administrative Manual, Section 4842, as the process of taking actions to avoid or reduce risk to acceptable levels.

A risk is a potential uncertainty, undesirable occurrence and/or unplanned event that could jeopardize one or more business processes. Risks to business processes should be assessed by category and by classification. Risks can be managed through identifying and prioritizing those risks deemed significant to a critical or necessary business function.

Figure A.1 portrays the **risk management** process.

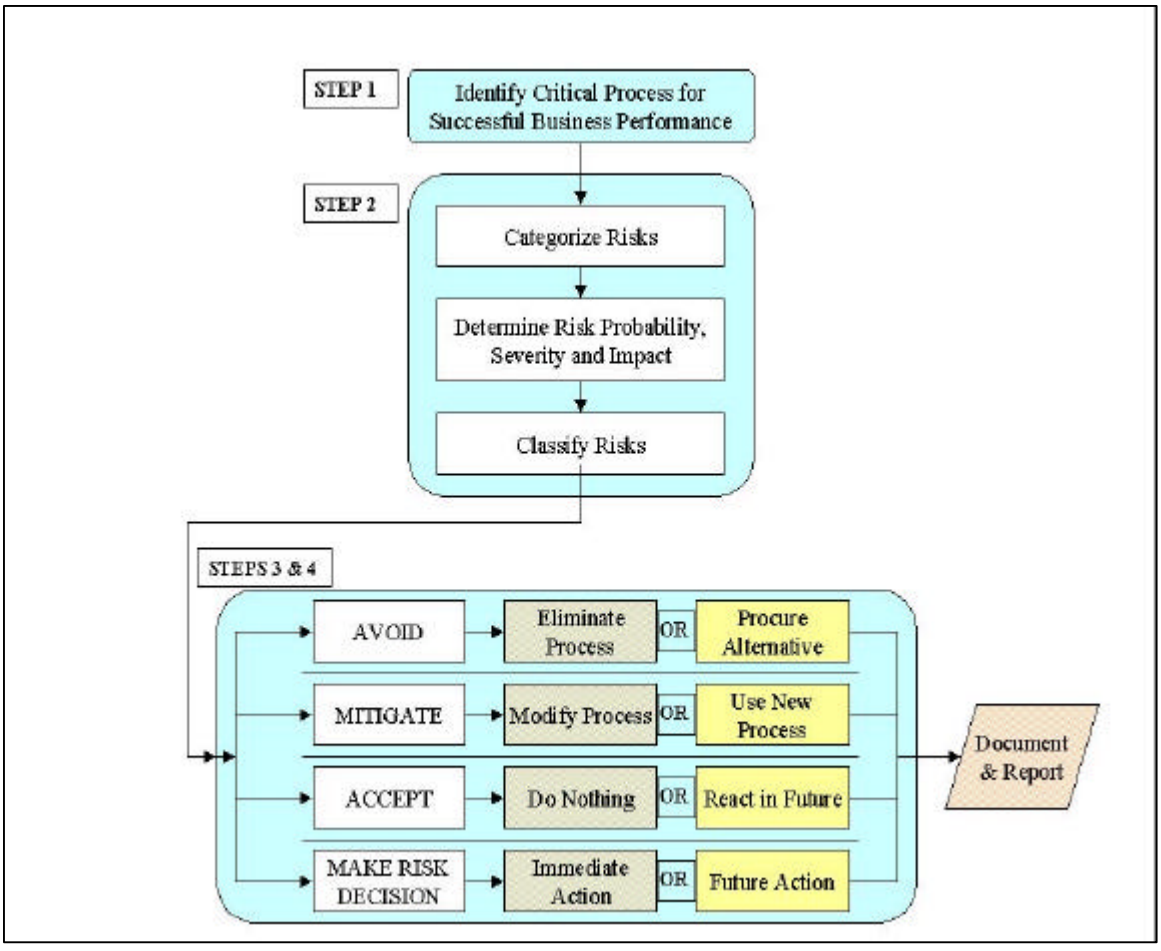

Figure A.1 - Risk Management Process

Risks can be reduced to an acceptable level by following these risk management steps:

1. Identify potential business risk areas

2. Determine the nature of the risks
   a) categorize the potential risk to necessary business processes
   b) determine the probability of the risk occurring
   c) assess the severity and impact of the risk, if not contained within an acceptable time frame
   d) classify the risk as high, medium, or low

3. Develop a risk management plan
   a) mitigate the likelihood of the risk occurring, or
   b) degrade the nature of the risk, or
   c) provide for contingencies in the event the risk occurs

4. Manage the risk so it will have a minimal or low impact to the overall performance of the necessary business functions

A.1: Identify potential business risk areas

The proper development of a risk management process takes all potential risks into consideration. Reviewing the following list of support areas will provide invaluable information and assessment data regarding the various aspects of the business. Any or all of these areas may be dependent upon the desktop for daily support of necessary business functions:

- Accounting
- Contract Management/Administration
- Financial Management
- Labor Relations
- Property Management
- Safety
- Configuration Management
- Environmental
- Human Resources
- Program Management
- Public Service
- Policy Development

The specific types of risks that should be considered as potentially impacting the desktop's support of necessary business functions can be derived from these areas.

A.2: Determine the nature of the risk

The level of risk must first be determined. For the purposes of this effort, risks have been grouped as high, medium, and low.

A **high** risk is defined as one that, if triggered, would cause a critical or necessary business function to fail. In the event of the failure of a critical or necessary business process, immediate actions would be required to correct the problem. Parallel or backup operations would be required to ensure continuation of the business process.

A **medium** risk is defined as one whose impact may be potentially significant in terms of resources, time, and/or cost of maintained performance of the business function. Failure of a significant business process by a medium risk would require expeditious and direct response towards resumption of operations.

A **low** risk is defined as one that is not known to appreciably impair the overall success or performance of the critical or necessary business function. Low risk areas, such as marginal or low-level business operations, equally carry the low risk designation.

One tool for determining the nature of the risk is the Assessment Report: a table of necessary business process areas wherein risk levels are assigned and high-level definitions of the risk and its associated solution are identified. A sample assessment report is presented in Table A.1.

Necessary Process Area	Level of Risk	OBSERVATIONS	Corrective Actions
Cashiering	High	Present software release calculates inaccurate date information and posts incorrect totals to customer data file.	Procure software upgrade.
Employee Time Logging	Medium	Present software stores data in 2-digit format; calculates leave inaccurately.	Modify application code.

Table A.1 - Sample Assessment Report

Once risks have been identified, a first step towards prioritized remediation is categorization. Desktop systems with the greatest risk of affecting necessary business functions can be categorized as follows:

- Category 1 - **Health and Safety**: where the loss or degradation of these systems could jeopardize the health and safety of California State employees or the public, or the safety of State property or private property.
- Category 2 - **Environmental Impact**: where the loss or degradation of these systems could negatively impact the environment within the State of California.
- Category 3 - **Operational Impact**: where the loss or degradation of these systems could negatively impact the ability of a department to perform its missions.
- Category 4 - **Public Confidence**: where the loss or degradation of these systems could cause the public to lose confidence in the State's government.
- Category 5 – **Other**: systems that are not categorized above.

When systems can be categorized into more than one category, assign the system to the highest applicable category.

Additional tools, such as the Risk Assessment Worksheet in Table A.2, can also be used to great effect in defining and documenting risks to necessary business functions. The Risk Assessment Worksheet, when used as a prioritization tool, will make possible a more focused remediation effort, given the potential level of substantiation inherent within the document.

Risk Category:				
Identification and description of risk:		**High**	**Medium**	**Low**
	Impact of Risk			
	Severity of Risk			
	Probability of Risk			
	Aggregate of Risk			
Urgency of handling the risk:	**Urgent Action:** 1 – 2 day response rate **Normal Action:** 3 – 5 day response rate **Low Action:** 2 – 4 weeks response rate			
Why is this a risk?				
What will happen if the risk is not contained?				
What is the trigger for this risk to occur?				
Contingency plans for containing the risk:				
Estimated cost associated with preventing the risk:				
Estimated cost if the risk is not contained:				

Table A.2 - Risk Assessment Worksheet

A.3: Develop a risk management plan

Targeted risk areas must be identified and those actions required to mitigate the risks must be documented and maintained. Prioritized risk areas will require prioritized attention. To mitigate the risk, specific actions including inventory, assessment, remediation, and testing of desktop systems with potential Y2K problems may be necessary. The accurate monitoring and managing of the overall remediation process is contingent upon careful planning of activities associated with risk mitigation.

Once the types of activities have been determined, scheduling those activities must occur along with a determination of resource requirements necessary, both personnel and hardware/software. Obtain front-end authorization for managing the anticipated effort, including best estimates of associated costs. Costing will be difficult at this early stage, but these figures can be refined as the remediation process progresses.

A.4 Manage the risk

Managing identified risks to necessary business functions is a straightforward process, employing similar methods as managing any other time-sensitive activity: watch resource commitments/requirements, budgetary, and schedule issues, and adjust when necessary.

Managing risks not previously identified is a much more difficult task, expending even more time and money. The best alternative to dealing with a new risk to necessary business functions would be to follow the same methodology as described within this document. This methodology was specifically developed to be responsive to a short timeframe process, which would be precisely what is encountered in managing an unexpected risk.

APPENDIX B: AUTOMATED TOOL SETS

Various automated tool sets are available to aid in assessing the scope and nature of the Y2K problem on the desktop. Many tools work across a variety of platforms and configurations, and most have a significant history of use in the marketplace. These tools can be viewed as servicing specific desktop environmental problems, such as BIOS timers, operating systems, or spreadsheets. The following paragraphs describe the current world of automated assessment tools.

> ***CRITICAL SUCCESS FACTOR: Select and employ an appropriate set of automated tools. This will bear great payback in terms of remediation as well as in management of the process.***

B.1 Available Tools per Hardware/Software Type

A multitude of commercial tool sets is available to assist across the full range of desktop Y2K issue areas. The industry has compartmentalized or subdivided many of these tools in terms of capabilities in the following areas:

- Inventory
- Assessment
- Remediation
- Repair
- Test Generation
- Test Analysis

For a review of tools available across this range of function, see Table B.1.

> Disclaimer: The DOIT has not made any assessment nor performed any tests verifying the suitability or non-suitability of any products listed herein as to their advertised purpose. The DOIT has made every effort to ascertain the validity of a product's existence and market presence. Because of the tremendous variety in desktop environments throughout the state, the task of establishing the suitability or validity of a tool to a particular purpose must be borne by the using organization.

B.2 Criteria for Evaluation of Applicable Tools

The selection of tools, whether identified on the table below or otherwise, should be based upon the following non-prioritized considerations:

1. Most critical area of need
2. Cost per unit
3. Vendor/product reputation
4. Likelihood of tool's success
5. Availability of internal/external human resources to implement tool

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
Accerl8 Technology Corporation Phone: (303) 863-8088 Email: mark.murphy@accelr8.com	Navigat8 - 2000 Solution 2000		✓				✓					C, C++, COBOL, DCL, FMS, FORTRAN, VisualBASIC
Accelr8 offers turnkey Year 2000 tools and services for the DEC VAX/VMS, Alpha, UNIX, and NT user. Accelr8 offers Year 2000 factory service and on site assessment services.												
Air System Technologies, Inc. Phone: (500) 448-9660 Email: indoor@airsystem.com	RighTime					✓						BIOS,DOS, Windows
Correct the CMOS Real Time Clock Y2K problem												
AMS Group International Distributors, Inc. Phone: (414) 352-4896 Email: Sales@2000tools.com Web Site: www://2000tools.com	Suite	✓	✓	✓	✓	✓	✓			✓	✓	Windows Access, Paradox, Foxpro, Excel, Lotus 123
Graphical set of tools running under Windows 3x, 95 and NT. Scalable from single PC to multiple mainframe environments. Programs identifying dates which are not Year 2000 ready. Searches PC, midrange and mainframe databases, spreadsheets and other file types.												
Aonix, Inc. Phone: (415) 543-0900 (800) 97-Aonix Web Site: www://aonix.com	StP/T							✓	✓			UNIX, NT Ada, C++, Java
The main objective of the 10X Program is to implement a tool-assisted testing process that will reduce time-to-test by at least a factor of 10 and will increase the quality of test coverage by at least tenfold. The services include management and technical consulting and training courses. Software modeling and testing tools complete the package.												
ArchiData Systems, Inc. Phone: (714) 282-7833 Email: DataMan911@AOL.COM Web Site: www://archidatasystems.com	ArchiMan Approximate Cost: $4900	✓	✓			✓	✓					OS2, C, C++, CICS, COBOL, DDL, PowerBuilder, RPG, Visual Basic
ArchiMan is a rule-based system that is platform independent. It scans the source building a repository for every line read and builds indexes to those lines matching the Y2K rules; thus, allowing correction of code after the assessment phase.												
AutoTester Phone: (800) 328-1196 (214) 368-1196 Web Site: www://autotester.com	Distributed Test Facility									✓	✓	OS/2, Windows
AutoTester offers immediate year 2000 testing productivity with an easy to use test creation facility. You can create, document, and execute automated tests for a variety of graphical interfaces. AutoAdviser serves as a central test repository and manages the quality assurance process of your year 2000 testing projects throughout their testing lifecycle. AutoController verifies the performance of the application under load conditions.												
Avatar Systems Phone: (800) 393-1313 Email: avatar@avatars.com Web Site: www://avatars.com	Suite			✓	✓	✓	✓					All source code assessment (more than 40 languages) including 4GLs, Windows COBOL, DBMSs
Product is a language and environment independent custom toolset providing a three-base approach to assess, plan and execute required changes.												
BDM International, Inc. Phone: (703) 848-7150 (800) 794-6085 Web Site: www://bdm.com	SMART Validator										✓	MVS, AS/400 COBOL, JCL, Natural, AL, C, PL/I
Provides an enterprise-wide approach to validate renovated applications, associated software, hardware systems and interfaces, and non-information systems that are currently in production and could be date-sensitive.												

Table B.1 - COTS Tools

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
BindView Dev. Corp. Phone: (800) 749-8439 email: info@bindview.com Web Site: www://bindview.com	NETinventory		✓				✓				✓	PC DOS, Windows spreadsheets, files, DBs
NETinventory is a modular solution for System management and Inventory analysis. Developed particularly for large Multi Site of networks. Testing modified applications for year 2000 projects, duplicate functionality for an entire enterprise-wide network with NETinventory and analyze in parallel with continuing repair, and receive thereby important support safe, strategic contingency options.												
Blair and Associates, Inc. Phone: (804) 633-4586 Email: jlhunt@huntmark.com	The Slicer Approximate Cost: $995.00 + $.20/line of code	✓	✓	✓	✓	✓	✓	✓	✓			Windows C, FORTRAN
Enables the user to identify, analyze, remediate, and test software problems, including the Y2K problem. Offers a 1.5 to 4x improvement in productivity over using manual methods.												
CACI International, Inc. Phone: (703) 841-3720 Email: npeters@hq.caci.com Web Site: www://year200.caci.com	RESTORE 2000	✓	✓	✓	✓	✓	✓	✓	✓			UNIX COBOL, C++, SQL
Software development processes at CACI have been independently certified as being at SEI Level 3 Compliant. The Restore 2000 methodology applies a comprehensive three-phase process to client information systems. Restore 2000 is certified by the ITAA as meeting the highest standards of Y2K compliance.												
Caldera Phone: (801) 765-4906 Web Site: www://caldera.com	DR-DOS 6.0					✓						BIOS
Dr. DOS is a disk operating system. With a kernal that will correct the system date even if your BIOS does not.												
Cayenne Software Phone: (800) 285-7294 (617) 273-9003 Web Site: www://cayennesoft.com	Cayenne 2000			✓	✓		✓	✓	✓			Sun, VMS, HP/UX, OS/2, DOS, Windows COBOL
Offers advanced analysis and migration support. Cayenne 2000 is its Y2K-specific COBOL analysis and repair tool, which provides objective diagnosis of Y2K problems, detects date dependencies across multiple programs, and corrects many of the simpler problems it finds. It also confirms any fixes made as a double check.												
CDG 2000, Inc. Phone: (403) 531-9030 Email: nasserf@cadvision.com Web Site: www://cadvision.com/cdg/cdg2000/profile.html	2000 PC assessment			✓								DOS, Windows
A combination of automation tools and engineering services designed to assist in identifying, documenting, and quantifying Year 2000 date remediation requirements. A comprehensive PC technology that will automatically assess the magnitude of your Year 2000 problem on user-developed applications, third-party software, spreadsheets, databases, data files, and in-house source code. Additionally, CDG 2000, Inc. is marketing a PC century clock correction software package.												
Cognizant Technology Solutions Phone: (212) 887-2385 Web Site: www://cts-us.com	CTS 2000				✓		✓		✓			COBOL, PL/1, Assembler, Model 204, Visual Basic, C, C++, Power Builder, Embedded SQL
Full spectrum solutions to handle the year 2000 problem right from assessment to implementation -- on mainframe and client-server platforms. The CTS 2000 toolset automates various stages of the year 2000 project life cycle.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
Computer Experts, Ltd. Phone: +44 1273 696975 Web Site: www://computerexperts.co.uk/pc2000	Millennium Bug Toolkit			✓		✓						PCs
Tests the RTC-BIOS 2000 interface, this is the safest system for protecting data & software. The Millennium Bug Toolkit runs completely from the floppy disk drive and does not interact with your hard disk during the testing procedure. This solves the problem of potentially different results which can come from virtually identical BIOS.												
C'QUEST International, Ltd. Phone: +44-(0)-1344-23069 Email: cquest@dial.pipex.com Web Site: www://cquest2000.com	Conversion Workbench				✓		✓					OS/2, DB/2, Windows NT, MVS, AS/400, VMS, Honeywell, HP, HP3000, ICL, Prime, Siemens, Unisys FORTRAN, FOCUS, JCL, MARK IV, COBOL, PL/I, Natural, Quiz, Quik, QTP, RPG, SAS, Schema, MODEL 204, TELON, IMS, SQL
Offers a robust, cost-effective toolset for the analysis and conversion of legacy software, supporting most platforms and languages. Available for IT companies, system integrators, consultants and end-users. CWB has been used to successfully process over one billion lines of code and also supports the Euro conversion. International languages (German, French, Spanish, Portuguese, etc.) are also supported.												
Diamond Optimum Systems Web Site: www://diamondos.com	D-Day 2000		✓		✓							HP/3000, MPE, Windows programs, jobs, files
A collection of reports used to identify programs, job streams and other files that may be affected by the Century Date Change (a.k.a. Y2K) problem. D-Day 2000 uses the client/server technology to produce a series of Decision Support Graphs (DSG) on an MS Windows workstation.												
Dortech Electronics, Ltd. Phone: +44 1202 776302 Web Site: www.//dortech.demon.co.uk/	Millennium BIOS Board . Cost is #59.99 (Pounds Sterling).					✓						BIOS
Plug in BIOS extension board for IBM PC's using 8086 to Pentium processors (or 100% compatible). Requires only an ISA slot. Firmware loads at start-up to correct year 2000 fault. Tested with all known BIOS.												
EasiRun, Inc. Web Site: www://easirun.com	ADAPT/2000			✓	✓	✓	✓					OS/390, UNIX, VMS, Windows, DOS COBOL
ADAPT/2000 provides a workstation-based approach, allowing source code and data to be offloaded for Year 2000 adaptation. Data is accepted in flat sequential format, with either EBCDC or ASCII encoding. The A2K Date Library, with over 50 routines for date conversion, arithmetic, display formatting and validation, with a rolling 10,000 year window, and user-defined cutoff year for date conversion.												
EraSoft Phone: (403) 248-2736 Web Site: www://erasoft.com/y2k/	Suite	✓		✓		✓						BIOS
EraScan PC detects and reports potential spreadsheet date problems. Clearly identify dates near a conversion cusp, dates that will change value with a software upgrade, and any functions that directly or indirectly reference problematic cells.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
G. R. Helm, Inc. Phone: 01-916-933-9669 Email: Gordon Helm year2000@grhelm.com Web Site: www://grhelm.com	Time Shift 2000 Cost of license is $2,900.				✓							HP 3000, MPE/iX, MPE/XL, MPE/V, Windows, PCs
Tool developed at GRHI and will both 'analyze' and 'age' date data fields in an IMAGE database. This software has been designed to automatically find and examine all date fields contained in a database. Reports the number of records found for each year encountered, the number of any unknown date values and the location of the date field within the field, when date fields are concatenated within other fields. 'aging' feature allows the user to increment any of the IMAGE date fields by some number of years (positive or negative). TS2000 process dates by their IMAGE field name but also allows the user to exclude fields from particular sets.												
Greenwich Mean Time Phone: (703) 908-6643 Email: Bruce Watenpaugh watenpab@utanet.com Web Site: www://gmt-2000.com	Check 2000 PC Citeck 2000 Client	✓	✓									PC Windows
Check 2000 PC performs a detailed hardware and shrink wrapped software audit of your PC to identify where year 2000 problems lie. Identifies CPU type, operating system, number of drives, hard disk size, and free space, shrink wrapped software programs and compares each one with our year 2000 knowledge base for year 2000 date dependencies. Identifies data known to be particularly date sensitive, such as that contained in databases and spreadsheets, and detailing when they were last accessed to help you prioritize on the most important problems first. Performs six hardware level BIOS checks, including whether the PC will successfully rollover from December 31, 1999 to January 1, 2000.												
i-Logix, Inc. Phone: (908) 528-1239 Web Site: www://ilogix.com	StateMate								✓			AIX, HP, SunOS, VMS Ada, C, C++
StateMate tools support static and dynamic analyses of systems and generation of documentation and programs, including requirements traceability through all stages of implementation.												
Information Builders, Inc. Phone: (800) 969-4636 Web Site: www://ibi.com	FOCUS		✓									VMS databases
Interpretes 2-digit year dates in existing applications and databases, offers outstanding flexibility for managing the definition, maintenance, and use of dates.												
IPL, Ltd. Phone: +44-(0)1225-475000 Web Site: www://iplbath.com	AdaTEST										✓	UNIX Ada
Software verification products which offer a complete and cost effective solution to the verification of these languages. Test harnesses and scripting tools work by allowing users full control of the interface between the software under test and the rest of the system. This means that any call from the class under test can be isolated from other parts of the system or utilise the real software as selected by the tester. This puts the tester firmly back in control of the test - not driven to compromise by the architecture of the language.												
ITCN Phone: (513) 439-2648	TD2000											DOS, UNIX
A solution for testing subsystems with simulated timing.												
LAN Supervision Inc. San Ramon, CA www.lsvi.com	Enterprise Inventory Auditor, Change Mgmt. Facility		✓		✓							Novell, Win95, WinNT, System 7
Comprehensive inventory and asset management system. Checks BIOS ans software versions; maintains database of asset management information.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
McCabe & Associates Phone: (800) 638-6316 FAX: (410) 995-1075 Web Site: www:/mccabe.com	Visual 2000 Environment			✓	✓			✓	✓			Windows 3.x, 95, NT, UNIX, VMS, DOS, Windows, OS/2 Ada, C, COBOL including mainframes, FORTRAN, Jovial
A visual, interactive toolset and methodology used by professional software engineers to bring computer systems into year 2000 compliance. Providing an interactive environment where you can analyze, remediate and test software for compliance with the year 2000 requirement.												
Mecury Interactive Phone: (800) TEST-911 Email: info@merc-int.com Web Site: www://merc-int.com	Testsuite2000				✓		✓				✓	Win 3.1, Win 95, Win NT, UNIX
Automated Testing tools for Y2K for Mainframe, Client Server Applications, Load Testing, and Enterprise Wide Test Management to enhance the entire process from Assessment, Remediation and Testing. Provides an audit trail of where you are in the process, launches automated scripts, gathers testing data, produces reports and provides a bug tracking utility.												
MicroFocus Phone: (800) MFCOBOL (800) 872-6265 Email: rbn@microfocus.com Web Site: www://microfocus.com	Suite		✓		✓		✓		✓		✓	AIX, HP, DG COBOL, MVS, GCOS, Siemens COBOL, DB2, SQL, CICS, IMS
Identifies only those dates which require fixing, such as dates used in some calculations and comparisons. Windowing leaves the two-digit dates in place, but adds logic to differentiate between centuries. It covers a full range of Y2K project activities including application inventory analysis, Y2K assessment and estimating, complete date identification, impact analysis, and code modification. Workbench/2000 supports the development and maintenance of mainframe applications in a distributed environment that includes workstations, network servers, and mainframes.												
Microsoft, Inc. Phone: (206) 882-8080 Web Site: www:/microsoft.com	Microsoft Test									✓		Windows
Microsoft Test organizes test activities and coordinates results over several runs. Codeview supports Y2K testing by helping with path analysis and value tracing.												
Millennium Technologies Institute, Inc. Phone: (619) 660-2400 Email: KirkLafler@compuserve.com	MTI/ASSESSOR, MTI/FirstLook	✓	✓		✓							Data entry, MVS, VM, VMS, UNIX, DOS COBOL, FORTRAN, SAS
Uses a five-phase structured methodology combined with a series of Year 2000 products, services, and training. MTI/ASSESSOR(tm) captures inventory and survey activity using a series of comprehensive data entry forms and stores information in a protected repository for use in subsequent Y2K phases. MTI/FirstLook(tm) Scanner and Parser Tool scans COBOL, FORTRAN and SAS source code for date use and location. Identified areas include computations, comparisons, projections, and sorting using input and output picture clauses (templates), functions, and action statements. Date density and complexity reports are produced.												
New Art Technologies, Inc. Phone: (212) 362-0559 Email: jkeyes@business-america.com Web Site: www://newarttech.com	NA2000 SCAN (license is $595) , NATRACE (license is $295)			✓	✓			✓	✓			COBOL
A series of a Windows-based, interactive, language independent, re-engineering modification tools. Default search criteria file contains over 200 Year 2000 date-related criteria. Fuzzy search capabilities - ability to match at 75%, 50% and 25% levels between search criteria and code.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
Piercom, Ltd. Phone: +353-61-335322 Web Site: www://piercom.ie	Suite			✓	✓	✓	✓					More than 40 languages
Provides meaningful analysis of date-impacted applications. The software identifies all date occurrences and pinpoints the exact location of the affected source code across entire applications -not only is the location of each date field identified, but also how each date is used for definitions, date transfers, calculations or screens. A full metrics analysis is performed reporting on number and types of date occurrences, programs, files and databases affected, kernel representation and bridging impact , for scoping and management overview purposes. Results are outputted, using Hyper-linked documentation, in a colour-coded format for easy identification.												
Platinum Technology, Inc. Phone: (800) 426-0469 (800) 442-6861 Web Site: www://platinum.com	Suite				✓			✓	✓		✓	UNIX, Windows COBOL, DB2, MVS, AS/400 COBOL, DB2, PL/I
Offers complete y2k conversion using SystemVision2000 and TransCentury date routines. The service includes planning, impact analysis, editing, building and testing. TransCentury is a complete set of COBOL conversion routines. TransCentury File Age is a Y2K data aging software product useful for testing changed apps with simulated post millennium data. With File Age, it is not necessary for the user to write database conversion programs to accomodate changing date field formats. File Age converts dates following the user's choices of more than 150 date formats supported by TransCentury.												
Rational Software Phone: (408) 496-3600 Web Site: www://rational.com	Rational/Test, Purify										✓	UNIX, Windows, Windows95, WindowsNT, Ada, C, C++
Product family includes modern development methodology, data and process modeling, tools, education and training for today's software-development practices.												
Reasoning Systems Phone: (650) 429-0350 (888) FIX-4-Y2K Email: info@reasoning.com Web Site: www://reasoning.com	Reasoning/2000		✓				✓				✓	IBM,UNISYS,Solaris(R) Ada, COBOL, C, FORTRAN, JCL, PL/I
Reasoning/2000 for COBOL combines artificial intelligence and advanced compiler technology in a highly automated tool for analyzing and remediating COBOL source code and related objects. Reasoning/2000 for Inspection is a toolset and process used to automate the inspection of Cobol applications.												
Rigel Desktop Solutions Phone: 04 5627175 Web Site: www://rigel.co.nz	DateSpy Approximate Cost: $US250					✓						Windows 3.11, 95, NT, MS Excel
DateSpy is a Year 2000 assessment tool for Excel spreadsheets. Locates problems and supports fixing via use of Excel editing capabilities.												
Softbridge Phone: (800) 955-9190 Web Site: www://sbridge.com	ATF									✓	✓	OS/2, LANs
ATF's master test directory communicates with up to 50 systems through a LAN via a slave test driver running on hte same platform as the system under test. With a scripting language that can interleave commands to distinct systems under test it is possible to observe the behavior of each component and thus perform integration testing on the entire application.												
Software Emancipation, Inc. Phone: (781) 863-8900 Web Site: www://setech.com	DISCOVER			✓	✓	✓	✓	✓	✓			UNIX C, C++, SUN OS, SOLARIS, WINDOWS NT
DISCOVER Y2K is the Year 2000 solution for assessment, impact analysis, remediation, and testing of C and C++ software. It includes an Information Model, Impact Analysis, and Change Propagation. It consists of four application sets: REENGINEER/SET, DOC/SET, ADMIN/SET, and DEVELOP/SET, and is useful for finding and fixing Y2K problems.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
Software Engineering & Enhancement Center (412) 682-4991	COBOL Analyst				✓	✓	✓					MVS, OS/2, OS/90 COBOL, Windows COBOL
Provides diagrams automatically for system level program control flow, program structure charts, and DBD hierarchy. PC-based technology uses sophisticated pattern matching techniques, field analysis, and identification techniques. Application Dictionary provides ongoing value during assessment, as well as during the planning and conversion stages.												
Software Research, Inc. Phone: (800) 942-SOFT +1 (415) 957-1441 Email: miller@soft.com Web Site: www://soft.com	STW/REG, TDGEN, STW/COV							✓	✓	✓	✓	UNIX, Windows
TestWorks is a suite of test tools providing basic support for many traditional testing strategies. Included are capabilities for source coverage analysis for given test sets, regression analysis of test results due to impact of changes, and integration of the results analysis with metrics analysis for greater understanding of the systemic causes of persistent problems during migration and maintenance activities. Branch coverage: unit testing, integration testing. Call-pair coverage: integration testing, system testing, test suite validation. Graphical annotation: all levels of code test completion browsing, analysis.												
Storage Technology Corporation Phone: (800) STORTEK (786-7835) Web Site: www://storagetek.com	Parallel storage systems											VM, MVS, UNIX, Windows NT
Storage management technology to support parallel y2k testing. Information storage solutions that combine high-performance tape drives, automated tape libraries, disk arrays, networking products, integrated software and consulting services.												
Sun Microsystems Federal Phone: US (800) 872-4786 Canada (800) 722-4786 Web Site: www://sun.com/y2000	Y2KABI				✓							SunOS, Solaris C, C++
Year 2000 support includes conventional development support and special path-oriented testing analysis. Using the ABI tool on existing applications, developers and users will be better able to identify separate software components with the tendency to fail due to date handling inconsistencies. Once a date related manipulation component has been identified as more failure prone, a higher level of scrutiny of the component - possibly an inspection of source code - can be performed.												
SUPERIOR IS Phone: (713) 524-8998	Superior:2000				✓		✓					MVS Assembler, CICS, COBOL, JCL, PL/I, SAIL, RPG, FOCUS, IDMS, ADABAS/Natural
Superior:2000 is a comprehensive combination of Renovation Methodology and Code Conversion tool. Automatic Source Conversion of the Entire Application Environment: Programs, Copybooks, JCL, IDCAMS, Sort Fields, DBD/PSB, etc. Automated Data Conversion, Bridging, Test Data Creation Programs.												
TechForce / COSMOS Phone: +31 23 56 22929 FAX: +31 23 5627052 GSM: +31 6 54275571 Web Site: www://cosmos2000.com	COSMOS				✓			✓	✓			COBOL, PL/I, C on any platform, CICS, ADS/0, TECON, JCL, Ass/370 on MVS, RPG on AS/4000, Pascal on VMS, Clipper on PCS
The toolset is programming-language independent and interfaces can be developed quickly for virtually any programming language. The year2000 analysis consists of three distinct steps: Inventory analysis - completeness, Impact analysis - metrics for planning, Detail analysis - exact location of dates and infections.												

Table B.1 - COTS Tools (con't)

COMPANY	PRODUCT	Inventory		Assessment		Repair		Test Generation		Test Analysis		Platform / Language
		PC	C/S	PC	C/S	PC	C/S	PC	C/S	PC	C/S	
Vector Software Services, Inc. Phone: (401) 295-5855 Email: wkm@vectors.com Web Site: www://vectortec.com	MAP2000, VSS-MAP2000, VectorCAST/2000 Approximate Cost: $6000		✓		✓							Unisys MAPPER, Unisys COBOL, UNIX client/servers
Scans your source code and automatically generates the test code necessary to build the test simulation environments (or test harnesses) required to isolate the individual software components that may have been modified during the conversion effort. Provides utilities to construct and execute test cases, generate reports to provide an audit trail of expected and actual results, and a simulation capability. The Virtual Date Utility provides the mechanism to simulate the system clock and allows each test case to be executed with a specified date and time. Because the system clock is not modified, companies can continue with day-to-day operations on the same hardware used for the Year 2000 conversion efforts.												
VIASOFT Phone: (800) 525-7775 (602) 952-0050 Web Site: www://viasoft.com	Suite	✓	✓			✓	✓	✓	✓			OS/2 COBOL, MVS COBOL, PL/I, RPG, Win95
Offers Y2K solutions for PC and client/server environments. Identifies problems in spreadsheets and databases. Providea hardware and software component assessment and interface repair and replacement to support overall compliance objectives. Offers flexibility in achieving year 2000 conversion compliance by providing a customizable combination of products and services.												
Xinotech Research, Inc. Phone: (612) 379-3844 Web Site: www://xinotech.com	Suite				✓		✓					IBM,Windows,Solaris CICS, COBOL, DDL, JCL, IMS, SQL, PL/I , DEC, HP
Provides solutions for the Year 2000 problem, integration to the common European currency Euro, and customer-specific problems. It supports impact analysis, and the automatic conversion of the following: COBOL programs, IMS and DB2 databases, sequential files, MFS and CICS forms, and JCL procedures. It can also be customized for other languages and scenarios.												
XPS Phone: (508) 949-7661 Web Site: www://xpsoft.com	Inventory 2000 Approximate cost: $395 to $18,000.	✓	✓									PC Windows, many languages
Inventory2000 generates a searchable repository of data elements, routines, data types, reference locations, etc.												
Year2000 Consultants Phone: 0044 171 928 3456 Email: timt@y2000fix.com	Datefind-y2k	✓										DOS, Windows spreadsheets (mainframes via ODBC)
A fully featured datafile scanner that scans database, spreadsheet and source code files for non compliant date references. It works primarily on PC based systems but is able to scan mainframe files via an ODBC driver. In addition to scanning for non compliants dates within data. Datefind-y2k is able to correct and cross reference any data deemed to be non compliant. This provides an exceptional useful tool when ensuring that valuable company data is fully year 2000 compliant.												
Zycad Corporation (800) 453-4035	DOORS								✓			UNIX SQL, SGML
Dynamic Object-Oriented Requirements System. Uses advanced object-oriented techniques to handle the complexity of large numbers of interlinked requirements. It can be used as a requirements- based test generator for Y2K problems.												

Table B.1 - COTS Tools (con't)

SITE IDENTIFICATION AND POINTS OF CONTACT

Start Date/Time: _____

Site Name: _____ Identification Code: _____	Other Identifier: _____
1. Organizational Data:	
a. Complete Postal Address:	_____ _____ _____
b. Agency/Organization Name:	
c. Organization having administrative control over your activity:	
d. When will your activity move?	☐ Not applicable ☐ Before 2000 ☐ After 2000
e. Please provide the new address, month and year of the move:	☐ Not applicable Date: _____ Address: _____ _____ _____
2. Points of Contact (POC)	
a. Manager	Title:
(1) Name	
(2) Organization Name	
(3) Telephone Number	CALNET: Commercial: ( )
(4) Fax Number	CALNET: Commercial: ( )
(5) E-mail Address	
b. Overall Site POC	Title:
(1) Name	
(2) Organization Name	
(3) Telephone Number	CALNET: Commercial: ( )
(4) Fax Number	CALNET: Commercial: ( )
(5) E-mail Address	

c. Functional POC	Title:
(1) Name	
(2) Organization Name	
(3) Telephone Number	CALNET: Commercial: ( )
(4) Fax Number	CALNET: Commercial: ( )
(5) E-mail Address	
d. Technical POC	Title:
(1) Name	
(2) Organization Name	
(3) Telephone Number	CALNET: Commercial: ( )
(4) Fax Number	CALNET: Commercial: ( )
(5) E-mail Address	
e. Bldg. Manager (if appropriate)	Title:
(1) Name	
(2) Organization Name	
(3) Telephone Number	CALNET: Commercial: ( )
(4) Fax Number	CALNET: Commercial: ( )
(5) E-mail Address	
3. User Data:	
a. Total number of users supported by your activity	Total
b. Total number of procurement users supported by your activity	Total
c. Total number of procurement users on your LAN	Total
d. Total number of other staff users on your LAN	Total
e. Number of remote dial-up users	Total

End Date/Time: _____

Figure C.1 - Site Identification and Point of Contact Worksheet

DESKTOP INVENTORY

Start Date/Time: _____

For each user, indicate the specific workstation characteristics. Make copies as necessary.

User Information:

Name: Last: _____ First: _____ MI: ___

Office Symbol: _____ Phone: _____

Job Series: _____ Title: _____

Workstation Configuration:

Property ID Number: _____ Purchase Date: ___/___/___

CPU Vendor Name: _____ Type: _____ (386, 486, etc.)

Number of CPUs: _____ Speed: _____ (MHz) RAM: _____ (MB)

Hard Drive Size: _____ (MB/GB) Hard Drive Free Space: _____ (MB/GB)

Operating System: _____ (MS-DOS, UNIX) Version: _____

Floppy drive capability: _____ (1.2 Mb, 1.44 Mb, both, other) CD-ROM: ☐ Yes ☐ No

Video Driver: _____ (VGA, SVGA, etc.) Monitor Size: _____ Video RAM: ___ _____

SIMM Type (i.e., 30 pin, 72 pin, etc.): _____

Ports: _____ (serial, parallel) Number of empty bays: _____

Bus Type: (i.e., IDE, EIDE, SCSI, etc.): _____

Network Card: _____ BIOS: _____ IP Address: _____

GUI Name: _____ GUI Version: _____

W/S Location: Bldg. _____ Room: _____

Shared W/S: Yes No With whom? _____

Server/s Connected to: _____

Figure C.2 - Desktop Inventory Worksheet

DESKTOP COTS SOFTWARE

Word Processing:			
Name:		Version/Release:	
Name:		Version/Release:	

Spreadsheets:			
Name:		Version/Release:	
Name:		Version/Release:	

E-Mail Package:			
Name:		Version/Release:	

Other Packages:			
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	

Figure C.3 - Desktop COTS Software Inventory Worksheet

DESKTOP DATABASES

Database Product Name: _____ Vendor Name: _____

Version/Release: _____

EC/EDI Capability ☐ Yes ☐ No

EC/EDI Translation Done Locally: ☐ Yes ☐ No ☐ Not Applicable

Database Environment (i.e., relational, object oriented, etc.): _____

Distribution Methodology (i.e, central, distributed, etc.): _____

CASE Tools Used: ☐ Yes ☐ No

Product Name: _____ Vendor Name: _____

Version/Release: _____

Data Dictionary Available: ☐ Yes ☐ No

Data Models Available: ☐ Yes ☐ No

Total Number of Data Elements Used: ____

Number of Data Elements Standardized in the DDDS ____

Site Unique Data Elements:

Number of Unique Data Elements: _____

Total Number of Data Elements in AIS: _____

End Date/Time: _____

Figure C.4 - Desktop Database Inventory Worksheet

NETWORK SERVERS

Start Date/Time:	
	Indicate the specific characteristics of each server. Make copies as necessary.

Server Configuration:

Property ID:			Purchase date:	/ /			
CPU Vendor Name:			Type:		(386, 486, etc.)		
Number of CPUs		Speed:		(Mhz)	RAM:		(MB)
Hard Drive Size:		(MB/GB)		Hard Drive Free:		(MB/GB)	
Operating System:		(MS-DOS, UNIX)		Version:			
Floppy Drive Capability:		(1.2 MB, 1.44 MB, both, other)		CD-ROM:	☐ Yes ☐ No		
Video driver:		(VGA, SVGA, etc.)		Monitor Size:		Video RAM:	
SIMM Type (i.e., IDE, EIDE, SCSI, other):							
Ports:		(serial, parallel)		Number of Empty Bays:			
Network Card:		IP Address:					
BIOS:							
GUI Name:		GUI Version:					
Server location: Bldg:		Room:					
Server being used as a router?	☐ Yes	☐ No					
Which Node(s) does the server belong to?							
Number of Users:							
Network Operating System Name:		Version:					
If Windows NT:	☐	Single Domain	☐	Master Domain			
	☐	Multiple Master Domain	☐	Other (Specify):			
If Windows NT: Is gateway services for Netware running?	☐	Yes	☐	No			

If Yes: Was setup done using Netware migration tool for NT?	☐	Yes	☐	No				
If NOS is Netware, describe hierarchical structure:								
If Netware: Is bindery emulation mode running?	☐	Yes	☐	No				
If NOS is UNIX, what type?	☐	HP/UX	☐	SCO	☐	LINUX		
☐ Solaris	☐	AIX	☐	AU/X	☐	Sun OS		
Using Domain Name Service (DNS)?	☐	Yes	☐	No				
If Solaris: Is Network Information Name Service (NIS)?	☐	Yes	☐	No				
What patches or service packs are installed?								
Describe what security is implemented:								
If post office server:	☐	Yes	☐	No				
Is Telnet server installed?	☐	Yes	☐	No				
Is FTP installed?	☐	Yes	☐	No				

Figure C.5 - Network Server Inventory Worksheet

SERVER COTS SOFTWARE

Word Processing:			
Name:		Version/Release:	
Name:		Version/Release:	

Spreadsheets:			
Name:		Version/Release:	
Name:		Version/Release:	

E-Mail Package:			
Name:		Version/Release:	

Other Packages:			
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	
Name:		Version/Release:	

Figure C.6 - Server COTS Software Inventory Worksheet

SERVER DATABASES

Database Product Name:				Vendor Name:				
Version/Release:								
EC/EDI Capability:	☐	Yes	☐	No				
EC/EDI Translation Done Locally:	☐	Yes	☐	No	☐	Not Applicable		
Database Environment (i.e., relational, object-oriented, etc.):								
CASE Tools Used:	☐	Yes	☐	No				
Product Name:				Vendor Name:				
Version/Release:								
Data Dictionary Available:	☐	Yes	☐	No				
Data Models Available:	☐	Yes	☐	No				
	Total Number of Data Elements Used:							
	Number of Data Elements Standardized in the DDDS:							

Site Unique Data Elements:

Number of Unique Data Elements: _____

Total Number of Data Elements in AIS: _____

End Date/Time: _____

Figure C.7 - Server Database Inventory Worksheet

LOCAL AREA NETWORKS

Start Date/Time:			
LAN ID:			
(Check all that apply)			
LAN TYPE:	☐ Segment	☐ Backbone	
	☐ Other (specify):		
TOPOLOGY:	☐ Token Ring	☐ Ethernet	☐ FDDI
	☐ Peer-To-Peer	☐ Other (specify):	
CABLE PLANT:	☐ 10BaseT	☐ 10BaseT (STP)	☐ 10BaseT (UTP)
	☐ 10Base2	☐ 10Base5	☐ 10BaseFL
	☐ RS232	☐ RS422	☐ Hyperchannel
	☐ Other (specify):		
MEDIA:	☐ Etherwire	☐ Twisted Pair (category: ☐ 3 or ☐ 5)	☐ Fiber
	☐ Wireless	☐ Other (specify):	
MODE:	☐ Single	☐ Multi	
	☐ Other (specify):		
PROTOCOLS:	☐ Netbeui	☐ NetBIOS	☐ TCP/IP
	☐ 802.2	☐ 802.3	☐ 802.5
	☐ 802.6	☐ SNA/SDLC	☐ Decnet
	☐ SAA	☐ APPN	☐ APPC
	☐ SPX/IPX	☐ Vines	☐ SONET
	☐ Other (specify)		
CHANNEL SPEED:	☐ 10 Mbps	☐ 16 Mbps	☐ 100 Mbps
	☐ 155 Mbps	☐ 622 Mbps	☐ (OC12)
	☐ Other (specify):		
MGMT PROTOCOLS:	☐ SNMP	☐ RMON	☐ RMON2
	☐ SNMPII	☐ Other (specify)	
FAULT TOLERANT LINKS:	☐ Yes	☐ No	

HUBS:	☐ Centillion	☐ Cabletron	☐ 3COM	
	☐ Other (specify):			
HUB Aggregate Bandwidth:				
HUB Management:	☐ Spectrum	☐ HP Openview	☐ Netview 6000	
PERCENTAGE OF UTILIZATION:				
		Under 30%	Average Time of Peak:	
		Over 30%	Average Time of Peak:	
		Over 40%	Average Time of Peak:	
		Over 80%	Average Time of Peak:	
		Unknown		
HOURS OF LAN OPERATION:				
BOTTLENECKS/PROBLEMS:				
OTHER COMMENTS:				

Figure C.8 - LAN Inventory Worksheet

INVENTORY OF LICENSED SOFTWARE								
SOFTWARE						LICENSES		
Name	Version	Type	Purchase Year			Number of Single User Licenses	Number of Users Covered by Multiuser licenses	Enterprise

End Date/Time: _____

Figure C.9 - Inventory of Licensed Software Worksheet